P-660HW-Tx v3

802.11g Wireless ADSL2+ 4-port Gateway

User's Guide

Default Login Details

IP Address	http://192.168.1.254
Admin Password	broadband1

Firmware Version 3.70
Edition 3, 11/2009

ZyXEL

www.zyxel.com

Copyright © 2009
ZyXEL Communications Corporation

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.

Note: It is recommended you use the web configurator to configure the ZyXEL Device.

- Support Disc

  Refer to the included CD for support documents.

- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

Documentation Feedback

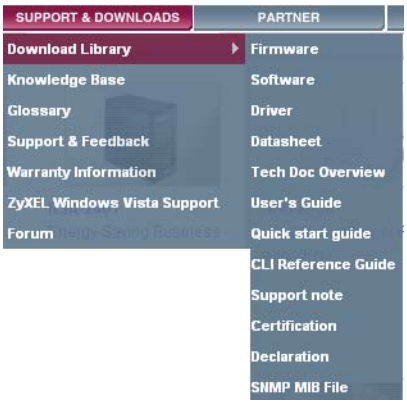
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Disclaimer

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated

firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

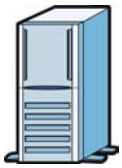
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-660HW-Tx v3 may be referred to as the "ZyXEL Device", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

ZyXEL Device	Computer	Notebook computer
Server 	Firewall	Telephone
Router	Switch	

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Contents Overview

Introduction **11**

Introducing the ZyXEL Device 23
Introducing the Web Configurator 31
Status Screens 37
Tutorials 47

Network **85**

Internet (WAN) Setup 87
Local Network (LAN) Setup 111
Wireless LAN 129
Network Address Translation (NAT) 163

Security **179**

Firewalls 181
Content Filtering 205
Packet Filter 211
Certificates 223

Advanced **231**

WAN IP Passthrough 233
Static Route 239
VLANs 243
Quality of Service (QoS) 253
Dynamic DNS Setup 275
Remote Management 279
Universal Plug-and-Play (UPnP) 289

Maintenance **301**

System Settings 303
Logs 309
Update/Reboot 323
Diagnostic 337
Statistics 339

Troubleshooting and Specifications **343**

Troubleshooting 345
Product Specifications 351

Appendices and Index 359

PART I
Introduction

Introducing the ZyXEL Device (23)

Introducing the Web Configurator (31)

Status Screens (37)

Tutorials (47)

Table of Contents

About This User's Guide 3

Document Conventions 6

Safety Warnings 8

Contents Overview 9

Part I: Introduction 11

Table of Contents 13

Chapter 1
Introducing the ZyXEL Device 23

1.1 Overview 23
1.2 Ways to Manage the ZyXEL Device 23
1.3 Good Habits for Managing the ZyXEL Device 24
1.4 Applications for the ZyXEL Device 24
1.4.1 Internet Access 24
1.5 LEDs (Lights) 26
1.6 The RESET Button 27
1.6.1 Using the RESET Button 27
1.7 The WIFI button 27
1.7.1 Turn the Wireless LAN Off or On 28
1.7.2 Activate WPS 28

Chapter 2
Introducing the Web Configurator 31

2.1 Overview 31
2.1.1 Accessing the Web Configurator 31
2.2 Web Configurator Main Screen 33
2.2.1 Title Bar 33
2.2.2 Navigation Panel 34
2.2.3 Main Window 36
2.2.4 Status Bar 36

Chapter 3
Status Screens 37

3.1 Overview 37
3.2 The Status Screen 38
3.2.1 Reset to Factory Defaults 40
3.2.2 Setting Up Remote Management for HTTP and Telnet 41
3.3 DHCP Client List 43
3.4 Wireless Clients 43
3.5 Any IP Table 44
3.6 Packet Statistics 45

Chapter 4
Tutorials 47

4.1 Overview 47
4.2 Setting Up a Secure Wireless Network 47
4.2.1 Configuring the Wireless Network Settings 48
4.2.2 Using WPS 49
4.2.3 Without WPS 54
4.2.4 Setting Up Wireless Network Scheduling 54
4.3 Setting Up Multiple Wireless Groups 55
4.4 Configuring the MAC Address Filter 59
4.5 Access the ZyXEL Device Using DDNS 61
4.5.1 Registering a DDNS Account on www.dyndns.org 61
4.5.2 Configuring DDNS on Your ZyXEL Device 62
4.5.3 Adding a Firewall Rule for Remote Management 62
4.5.4 Testing the DDNS Setting 64
4.6 Configuring Static Route for Routing to Another Network 65
4.7 Multiple Public and Private IP Address Mappings 67
4.7.1 Full Feature NAT + Many-to-Many No Overload Mapping 68
4.7.2 Full Feature NAT + One-to-One Mapping 70
4.8 ATM QoS and QoS Overview 71
4.8.1 Two PVCs with ATM QoS Scenario 71
4.8.2 Configuring QoS 76
4.9 Setting Up NAT Port Forwarding 82

Part II: Network 85

Chapter 5
Internet (WAN) Setup 87

5.1 Overview 87
5.1.1 What You Can Do in the WAN Screens 87
5.1.2 What You Need to Know About WAN 87
5.1.3 Before You Begin 88

5.2 The Internet Access Setup Screen 89
5.2.1 Advanced Internet Access Setup 92
5.3 The More Connections Screen 95
5.3.1 More Connections Edit 96
5.3.2 Configuring More Connections Advanced Setup 99
5.4 The WAN Backup Setup Screen 101
5.5 WAN Technical Reference 103
5.5.1 Encapsulation 103
5.5.2 Multiplexing 104
5.5.3 VPI and VCI 105
5.5.4 IP Address Assignment 105
5.5.5 Nailed-Up Connection (PPP) 105
5.5.6 NAT 106
5.6 Metric 106
5.7 Traffic Shaping 106
5.7.1 ATM Traffic Classes 107
5.8 Zero Configuration Internet Access 108
5.9 Traffic Redirect 109

Chapter 6
Local Network (LAN) Setup 111

6.1 Overview 111
6.1.1 What You Can Do in the LAN Screens 111
6.1.2 What You Need To Know About LAN 112
6.1.3 Before You Begin 113
6.2 The LAN IP Screen 113
6.2.1 The Advanced LAN IP Setup Screen 114
6.3 The DHCP Setup Screen 116
6.4 The Client List Screen 118
6.5 The IP Alias Screen 119
6.5.1 Configuring the LAN IP Alias Screen 120
6.6 LAN Technical Reference 121
6.6.1 LANs, WANs and the ZyXEL Device 121
6.6.2 DHCP Setup 122
6.6.3 DNS Server Addresses 122
6.6.4 LAN TCP/IP 123
6.6.5 RIP Setup 124
6.6.6 Multicast 124
6.6.7 Any IP 125

Chapter 7
Wireless LAN 129

7.1 Overview 129

7.1.1 What You Can Do in the Wireless LAN Screens 129
7.1.2 What You Need to Know About Wireless 130
7.1.3 Before You Start 130
7.2 The AP Screen 131
7.2.1 No Security 133
7.2.2 WEP Encryption 134
7.2.3 WPA(2)-PSK 135
7.2.4 WPA(2) Authentication 136
7.2.5 Wireless LAN Advanced Setup 138
7.2.6 MAC Filter 139
7.3 The More AP Screen 140
7.3.1 More AP Edit 141
7.4 The WPS Screen 143
7.5 The WPS Station Screen 144
7.6 The WDS Screen 145
7.7 The Scheduling Screen 147
7.8 Wireless LAN Technical Reference 147
7.8.1 Wireless Network Overview 148
7.8.2 Additional Wireless Terms 149
7.8.3 Wireless Security Overview 150
7.8.4 Signal Problems 153
7.8.5 BSS 153
7.8.6 MBSSID 154
7.8.7 Wireless Distribution System (WDS) 155
7.8.8 WiFi Protected Setup (WPS) 155

Chapter 8
Network Address Translation (NAT)..... 163

8.1 Overview 163
8.1.1 What You Can Do in the NAT Screens 163
8.1.2 What You Need To Know About NAT 163
8.2 The NAT General Setup Screen 165
8.3 The Port Forwarding Screen 166
8.3.1 Configuring the Port Forwarding Screen 167
8.3.2 The Port Forwarding Rule Edit Screen 169
8.4 The Address Mapping Screen 169
8.4.1 The Address Mapping Rule Edit Screen 171
8.5 The ALG Screen 173
8.6 NAT Technical Reference 173
8.6.1 NAT Definitions 173
8.6.2 What NAT Does 174
8.6.3 How NAT Works 175
8.6.4 NAT Application 176

8.6.5 NAT Mapping Types 176

Part III: Security 179

Chapter 9
Firewalls 181

9.1 Overview 181
9.1.1 What You Can Do in the Firewall Screens 181
9.1.2 What You Need to Know About Firewall 182
9.1.3 Firewall Rule for WAN Telnet Connection Example 182
9.2 The Firewall General Screen 186
9.2.1 Firewall Rules Overview 186
9.3 The Firewall Rule Screen 189
9.3.1 Configuring Firewall Rules 191
9.3.2 Customized Services 193
9.3.3 Configuring a Customized Service 194
9.3.4 Firewall Rule Using a Customized Service Example 194
9.4 The Firewall Threshold Screen 197
9.4.1 Threshold Values 198
9.4.2 Configuring Firewall Thresholds 198
9.5 Firewall Technical Reference 200
9.5.1 Guidelines For Enhancing Security With Your Firewall 200
9.5.2 Security Considerations 201
9.5.3 Triangle Route 201

Chapter 10
Content Filtering 205

10.1 Overview 205
10.1.1 What You Can Do in the Content Filter Screens 205
10.1.2 What You Need to Know About Content Filtering 205
10.1.3 Before You Begin 205
10.1.4 Content Filtering Example 206
10.2 The Keyword Screen 208
10.3 The Schedule Screen 209
10.4 The Trusted Screen 210

Chapter 11
Packet Filter 211

11.1 Overview 211
11.1.1 What You Can Do in the Packet Filter Screen 211
11.1.2 What You Need to Know About the Packet Filter 211

11.2 The Packet Filter Screen 212
11.2.1 Reset to Factory Defaults 212
11.2.2 Editing Protocol Filters 213
11.2.3 Configuring Protocol Filter Rules 214
11.2.4 Editing Generic Filters 216
11.2.5 Configuring Generic Packet Rules 217
11.3 Packet Filter Technical Reference 219
11.3.1 Filter Types and NAT 219
11.3.2 Firewall Versus Filters 219

Chapter 12
Certificates 223

12.1 Overview 223
12.1.1 What You Can Do in the Certificates Screens 223
12.1.2 What You Need to Know About Certificates 223
12.2 The Trusted CAs Screen 224
12.2.1 Trusted CA Import 226
12.2.2 Trusted CA Details 227
12.3 Certificates Technical Reference 229
12.3.1 Certificates Overview 229
12.3.2 Private-Public Certificates 229

Part IV: Advanced 231

Chapter 13
WAN IP Passthrough 233

13.1 The WAN IP Passthrough Screen 233
13.1.1 What You Need to Know About IP Passthrough 234

Chapter 14
Static Route 239

14.1 Overview 239
14.1.1 What You Can Do in the Static Route Screens 239
14.2 The Static Route Screen 240
14.2.1 Static Route Edit 241

Chapter 15
VLANs 243

15.1 Overview 243
15.1.1 What You Can Do in the VLANs Screens 243
15.1.2 What You Need to Know About VLANs 243

15.1.3 VLANs Example 245
15.2 The VLANs Group Setting Screen 249
15.2.1 Editing VLANs Group Setting 250
15.3 The VLANs Port Setting Screen 252

Chapter 16
Quality of Service (QoS) 253

16.1 Overview 253
16.2 QoS Overview 254
16.2.1 What You Can Do in the QoS Screens 254
16.2.2 What You Need to Know About QoS 255
16.2.3 QoS Class Setup Example 255
16.3 The QoS General Screen 259
16.4 The Class Setup Screen 260
16.4.1 The Class Configuration Screen 261
16.5 Traffic Shaping 265
16.6 Token Bucket 265
16.7 Token Bucket Example 266
16.7.1 The Queue Setup Screen 267
16.7.2 The Queue Configuration Screen 268
16.7.3 The QoS Monitor Screen 269
16.8 QoS Technical Reference 270
16.8.1 IEEE 802.1Q Tag 270
16.8.2 IP Precedence 271
16.8.3 DiffServ 271
16.8.4 Automatic Priority Queue Assignment 272

Chapter 17
Dynamic DNS Setup 275

17.1 Overview 275
17.1.1 What You Can Do in the DDNS Screen 275
17.1.2 What You Need To Know About DDNS 275
17.2 The Dynamic DNS Screen 276

Chapter 18
Remote Management 279

18.1 Overview 279
18.1.1 What You Can Do in the Remote Management Screens 280
18.1.2 What You Need to Know About Remote Management 280
18.2 The WWW Screen 281
18.2.1 Configuring the WWW Screen 283
18.3 The Telnet Screen 284
18.4 The FTP Screen 285

18.5 The DNS Screen 286
18.6 The ICMP Screen 287

Chapter 19
Universal Plug-and-Play (UPnP) 289

19.1 Overview 289
19.1.1 What You Can Do in the UPnP Screen 289
19.1.2 What You Need to Know About UPnP 289
19.2 The UPnP Screen 291
19.3 Installing UPnP in Windows Example 292
19.4 Using UPnP in Windows XP Example 295

Part V: Maintenance 301

Chapter 20
System Settings 303

20.1 Overview 303
20.1.1 What You Can Do in the System Settings Screens 303
20.1.2 What You Need to Know About System Settings 303
20.2 The General Screen 304
20.3 The Time Setting Screen 306

Chapter 21
Logs 309

21.1 Overview 309
21.1.1 What You Can Do in the Log Screens 309
21.1.2 What You Need To Know About Logs 309
21.2 The View Log Screen 310
21.3 The Log Settings Screen 311
21.4 SMTP Error Messages 314
21.4.1 Example E-mail Log 314
21.5 Log Descriptions 315

Chapter 22
Update/Reboot 323

22.1 Overview 323
22.1.1 What You Can Do in the Update/Reboot Screens 323
22.1.2 What You Need To Know About Update/Reboot 324
22.1.3 Before You Begin 325
22.1.4 Tool Examples 325
22.2 The Firmware Screen 331

22.3 The Configuration Screen 333
22.4 The Restart Screen 336

Chapter 23
Diagnostic 337

23.1 The Diagnostic General Screen 337

Chapter 24
Statistics 339

24.1 The Statistics General Screen 339
24.1.1 Terms 340

Part VI: Troubleshooting and Specifications 343

Chapter 25
Troubleshooting 345

25.1 Power, Hardware Connections, and LEDs 345
25.2 ZyXEL Device Access and Login 346
25.3 Internet Access 348
25.4 Network Connections 349

Chapter 26
Product Specifications 351

26.1 Hardware Specifications 351
26.2 Firmware Specifications 351
26.3 Wireless Features 355
26.4 Power Adaptor Specifications 358

Part VII: Appendices and Index 359

Appendix A Setting up Your Computer's IP Address 361
Appendix B Pop-up Windows, JavaScripts and Java Permissions 385
Appendix C IP Addresses and Subnetting 395
Appendix D Wireless LANs 405
Appendix E Services 421
Appendix F Legal Information 425
Index 429

1

Introducing the ZyXEL Device

This chapter introduces the main applications and features of the ZyXEL Device. It also introduces the ways you can manage the ZyXEL Device.

1.1 Overview

The P-660HW-Tx v3 is an ADSL2+ router. By integrating DSL and NAT, you are provided with ease of installation and high-speed, shared Internet access. The P-660HW-Tx v3 is also a complete security solution with a robust firewall and content filtering.

Please refer to the following description of the product name format.

- “H” denotes an integrated 4-port hub (switch).
- Models ending in “1”, for example P-660HW-T1, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in “3” denote a device that works over ISDN (Integrated Services Digital Network) or T-ISDN (UR-2).

Only use firmware for your ZyXEL Device’s specific model. Refer to the label on the bottom of your ZyXEL Device.

Note: All screens displayed in this user’s guide are from the P-660HW-T1 v3 model.

See the product specifications for a full list of features.

1.2 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP for firmware upgrades and configuration backup/restore.
- TR-069. This is an auto-configuration server used to remotely configure your device.

1.3 Good Habits for Managing the ZyXEL Device

Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

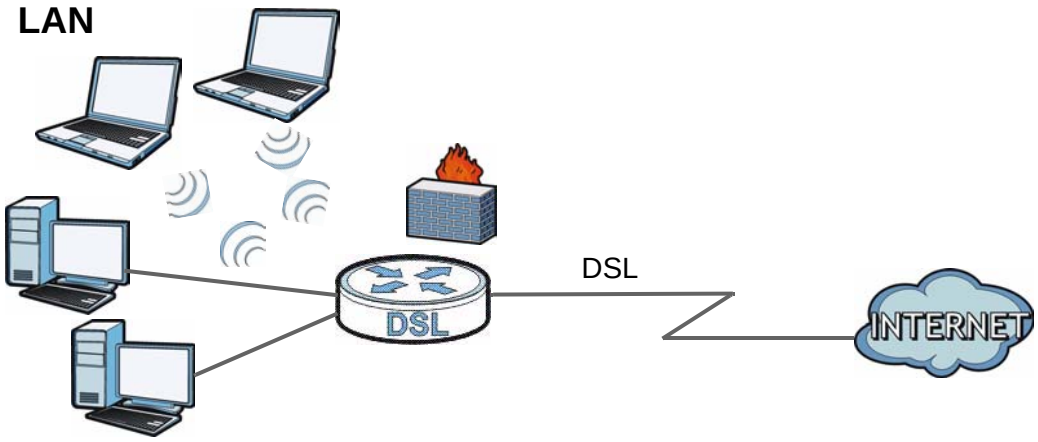
1.4 Applications for the ZyXEL Device

Here are some example uses for which the ZyXEL Device is well suited.

1.4.1 Internet Access

Your ZyXEL Device provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. Computers can connect to the ZyXEL Device's LAN ports (or wirelessly).

Figure 1 ZyXEL Device's Router Features



You can also configure firewall and content filtering on the ZyXEL Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

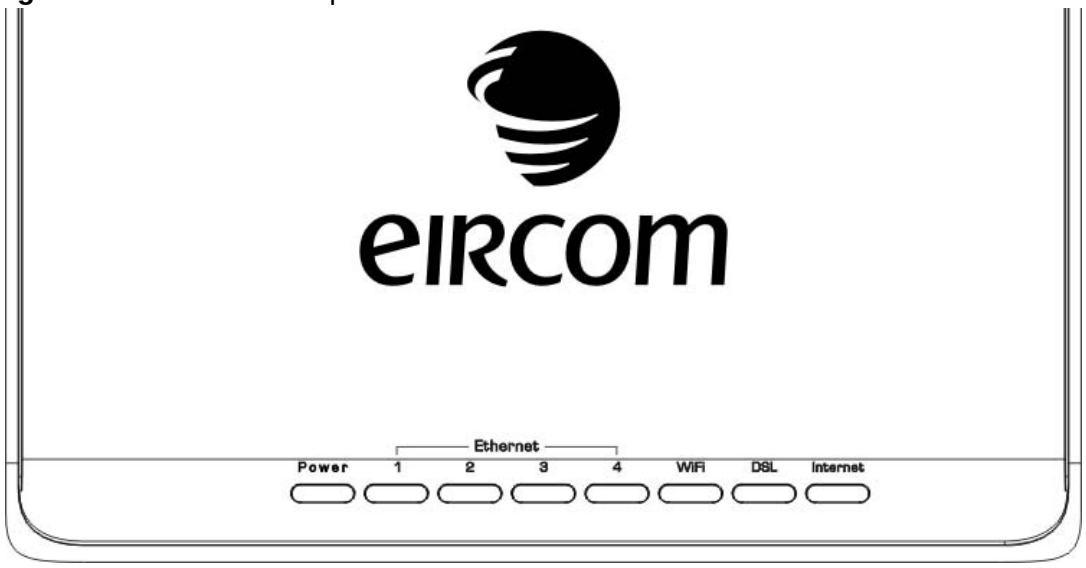
Use content filtering to block access to specific web sites, with URL's containing keywords that you specify. You can define time periods and days during which content filtering is enabled and include or exclude particular computers on your network from content filtering. For example, you could block access to certain web sites for the kids.

Use QoS to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers. For example, you could make sure that the ZyXEL Device gives voice over Internet calls high priority, and/or limit bandwidth devoted to the boss's excessive file downloading.

1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 2 LEDs on the Top of the Device



None of the LEDs are on if the ZyXEL Device is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
Power	Green	On	The ZyXEL Device is receiving power and ready for use.
		Blinking	The ZyXEL Device is self-testing.
	Red	On	The ZyXEL Device detected an error while self-testing, or there is a device malfunction.
		Off	The ZyXEL Device is not receiving power.
LAN 1-4	Green	On	The ZyXEL Device has an Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The ZyXEL Device is sending/receiving data to /from the LAN.
		Off	The ZyXEL Device does not have an Ethernet connection with the LAN.
WiFi	Green	On	The wireless network is activated.
		Blinking	The ZyXEL Device is communicating with other wireless clients.
	Orange	Blinking	The ZyXEL Device is setting up a WPS connection after pressing the WIFI button for 1-2 seconds. When WPS connection has been configured successfully, the LED will become green.
		Off	The wireless network is not activated.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
DSL	Green	On	The DSL line is up.
		Blinking	The ZyXEL Device is initializing the DSL line.
		Off	The DSL line is down.
INTERNET	Green	On	The ZyXEL Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The ZyXEL Device is sending or receiving IP traffic.
	Red	On	The ZyXEL Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off	The ZyXEL Device does not have an IP connection.

Refer to the Quick Start Guide for information on hardware connections.

1.6 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to “broadband1”.

1.6.1 Using the RESET Button

1. Make sure the **POWER** LED is on (not blinking).
2. To set the device back to the factory default settings, press the **RESET** button for 5 seconds or until the **Power** LED begins to blink. Do not turn off the device while the reset is in progress! When the **Power** LED stops blinking and lights green, the defaults have been restored and the device restarts.

1.7 The WIFI button

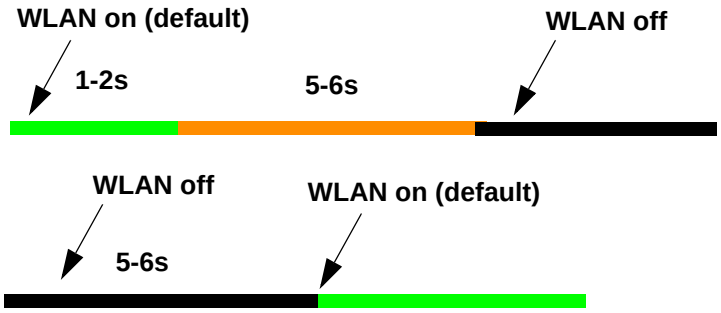
By default, the wireless LAN is on. You can use the **WIFI** button on the back of the device to disable or activate the wireless LAN. You can also use it to activate WPS in order to quickly set up a wireless network with strong security.

1.7.1 Turn the Wireless LAN Off or On

1 Make sure the **POWER** LED is on (not blinking).

2 The wireless LAN of the ZyXEL Device is enabled by default, so the LED lights green. If not, press the **WIFI** button for 5 to 6 seconds and release it when the LED turns green. The Wireless LAN is on. If you want to turn it off, press the WIFI button for 5 to 6 seconds again. The **WiFi** LED will initially turn to orange then turn off: release the button after the LED turns off.

Figure 3 Wireless LAN On/Off



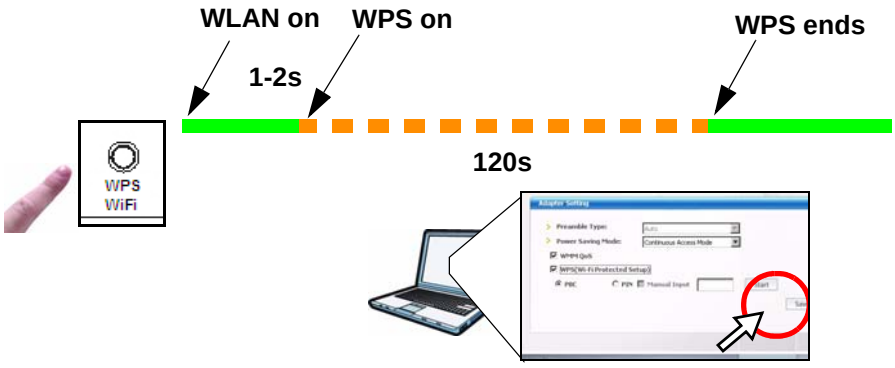
1.7.2 Activate WPS

1 Make sure the **POWER** LED is on (not blinking).

2 Check if the LED lights green (wireless LAN on). If not, press the **WIFI** button for 5 to 6 seconds and release it when the LED turns green. Then press the **WIFI** button again for 1 to 2 seconds and release it when the LED turns orange. Press the WiFi or WPS button on another WPS-enabled device within range of the ZyXEL Device. The **WiFi** LED should blink orange while the ZyXEL Device sets up a WPS connection with the wireless device. When the WPS connection has been configured successfully, the LED will become green.

Note: You must activate WPS in the ZyXEL Device and in another wireless device within 120 seconds of each other. See Section 7.8.8 on page 155 for more information.

Figure 4 Activating WPS



2

Introducing the Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

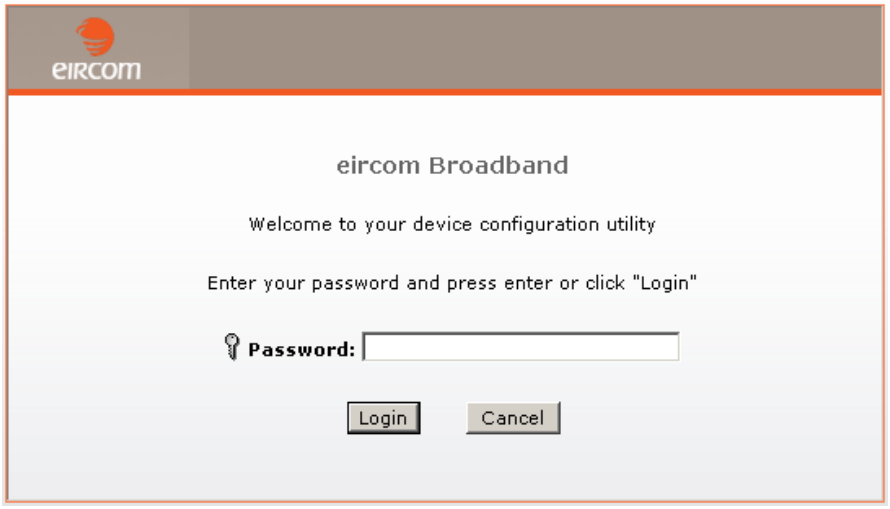
See Appendix B on page 385 if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

1. Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "http://192.168.1.254" as the URL.

4 A password screen displays. Type the admin password (broadband1 by default) in the password screen and click **Login**. Click **Cancel** to revert to the default user password in the password field. If you have changed the password, enter your password and click **Login**.

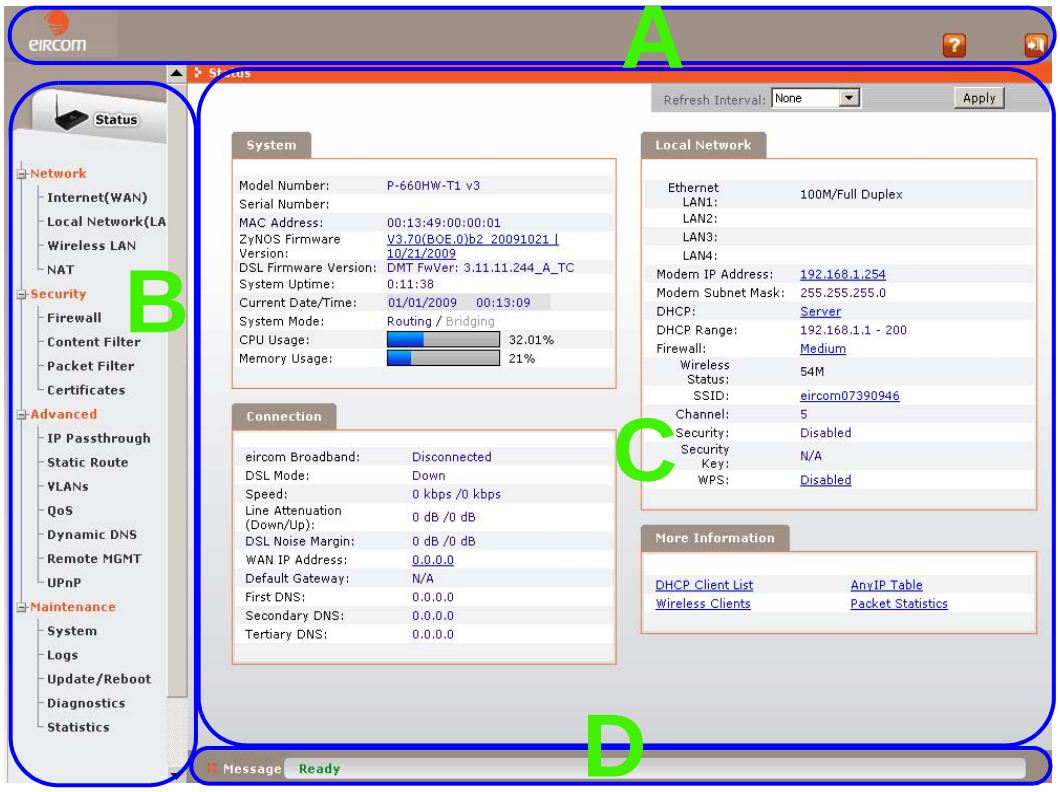
Figure 5 Password Screen



5 It is strongly recommended you change the default password. See Section 20.2 on page 304 for more information on changing password.

2.2 Web Configurator Main Screen

Figure 6 Main Screen

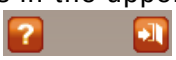


As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

2.2.1 Title Bar

The title bar provides some icons in the upper right corner.



The icon(s) provide(s) the following function.

Table 2 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	Help: Click this icon to open up help screens.
	Logout: Click this icon to log out of the web configurator.

2.2.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ZyXEL Device features. The following tables describe each menu item.

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen shows the ZyXEL Device's general device and network status information. Use this screen to access the statistics and client list.
Network		
Internet (WAN)	Internet Access Setup	Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
	More Connections	Use this screen to configure additional WAN connections.
	WAN Backup Setup	Use this screen to configure a backup gateway.
Local Network (LAN)	IP	Use this screen to configure LAN TCP/IP settings, enable Any IP and other advanced properties.
	DHCP Setup	Use this screen to configure LAN DHCP settings.
	Client List	Use this screen to view current DHCP client information and to always assign specific IP addresses to individual MAC addresses (and host names).
	IP Alias	Use this screen to partition your LAN interface into subnets.
Wireless LAN	AP	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	More AP	Use this screen to configure multiple BSSs on the ZyXEL Device.
	WPS	Use this screen to configure WPS (Wi-Fi Protected Setup) settings.
	WPS Station	Use this screen to set up a WPS wireless network.
	WDS	Use this screen to set up Wireless Distribution System links to other access points.
	Scheduling	Use this screen to configure the dates/times to enable or disable the wireless LAN.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to make your local servers visible to the outside world. This screen appears when you choose **SUA Only** from the **NAT** > **General** screen.
	Address Mapping	Use this screen to configure network address translation mapping rules. This screen appears when you choose **Full Feature** from the **NAT** > **General** screen.
	ALG	Use this screen to enable or disable SIP ALG.
Security		

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Firewall	General	Use this screen to activate/deactivate the firewall or set the firewall level.
	Rules	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule. This screen appears when you choose **Custom** from the **Firewall** > **General** screen.
	Threshold	Use this screen to configure the thresholds for determining when to drop sessions that do not become fully established.
Content Filter	Keyword	Use this screen to block access to web sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for your device to perform content filtering.
	Trusted	Use this screen to exclude a range of users on the LAN from content filtering.
Packet Filter		Use this screen to configure the rules for protocol and generic filter sets.
Certificates	Trusted CAs	Use this screen to save CA certificates to the ZyXEL Device.
Advanced		
IP Passthrough		Use this screen to enable IP Passthrough so one of your clients can share the same public IP address as the WAN side.
Static Route		Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
VLANs	Group Setting	Use this screen to activate 802.1Q/1P, specify the management VLAN group, display the VLAN groups and configure the settings for each VLAN group.
	Port Setting	Use this screen to configure the PVID and assign traffic priority for each port.
QoS	General	Use this screen to enable QoS and traffic prioritizing, and configure bandwidth management on the WAN.
	Class Setup	Use this screen to define a classifier.
	Queue Setup	Use this screen to configure QoS queues.
	Monitor	Use this screen to view each queue's statistics.
Dynamic DNS		This screen allows you to use a static hostname alias for a dynamic IP address.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the ZyXEL Device.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyXEL Device.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyXEL Device.

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyXEL Device.
	ICMP	Use this screen to set whether or not your device will respond to pings and probes for services that you have not made available.
UPnP	General	Use this screen to turn UPnP on or off.
Maintenance		
System	General	Use this screen to configure your device's name, domain name, management inactivity timeout and password.
	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Logs	View Log	Use this screen to display your device's logs.
	Log Settings	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Update/ Reboot	Firmware	Use this screen to upload firmware to your device.
	Configuration	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.
Diagnostic	General	Use this screen to test the connections to other devices.
Statistics	General	These screen displays information to help you identify problems with the DSL and Ethernet WAN connection.

2.2.3 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you connect to the URL, the **Status** screen is displayed. See Chapter 3 on page 37 for more information about the **Status** screen.

2.2.4 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

3

Status Screens

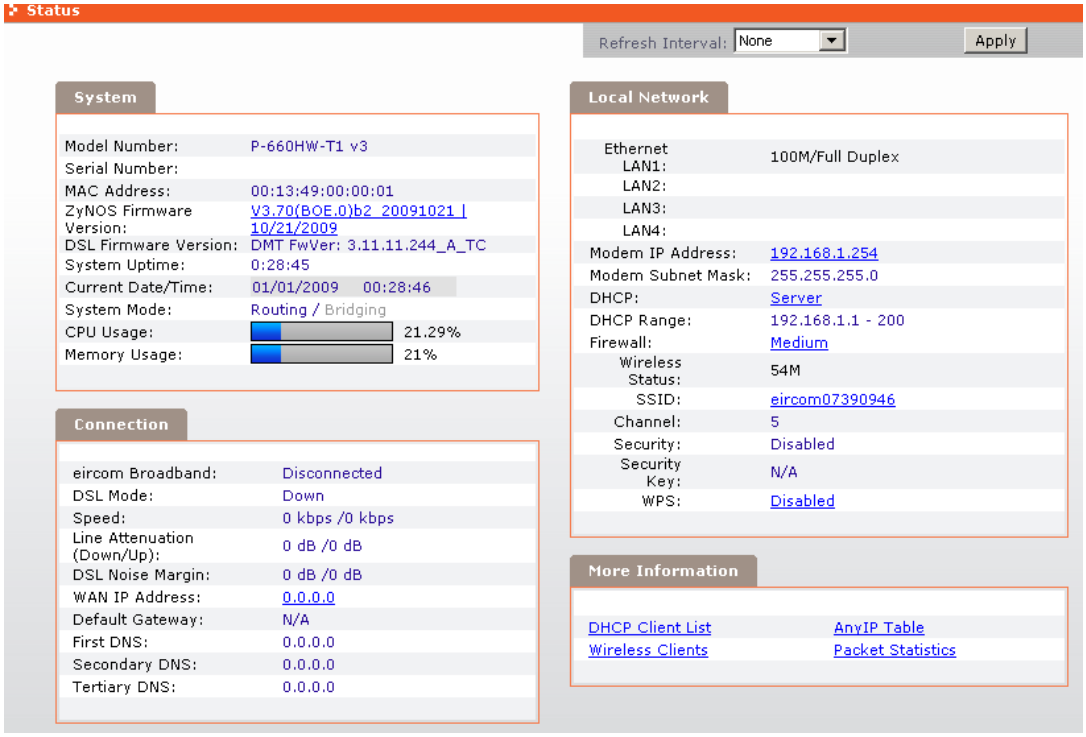
3.1 Overview

Use the **Status** screens to look at the current status of the device, system resources, and interfaces (LAN and WAN). The **Status** screen also provides detailed information from Any IP and DHCP and statistics from bandwidth management, and traffic.

3.2 The Status Screen

Use this screen to view the status of the ZyXEL Device. Click **Status** to open this screen.

Figure 7 Status Screen



Each field is described in the following table.

Table 4 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the ZyXEL Device to update this screen.
Apply	Click this to update this screen immediately.
System	
Model Number	This is the model name of your device.
Serial Number	This field displays the certificate's identification number given by the certification authority.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
ZyNOS Firmware Version	This is the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it.
DSL Firmware Version	This is the current version of the device's DSL modem code.

Table 4 Status Screen

LABEL	DESCRIPTION
System Uptime	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you plug it in, when you restart it (**Maintenance > Tools > Restart**), or when you reset it.
Current Date/Time	This field displays the current date and time in the ZyXEL Device. You can change this in **Maintenance > System > Time Setting**.
System Mode	This displays whether the ZyXEL Device is functioning as a router or a bridge.
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS; see Chapter 16 on page 253).
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the ZyXEL Device is probably becoming unstable, and you should restart the device. See Section 22.4 on page 336, or turn off the device (unplug the power) for a few seconds.
Connections	
eircom Broadband	This is the current status of your broadband.
DSL Mode	This is the DSL standard that your ZyXEL Device is using.
Speed	This is the speed of your DSL connection.
Line Attenuation	This indicates the line attenuation status for each upstream and downstream band.
DSL Noise Margin	This is the signal to noise ratio for the downstream part of the connection (coming into the ZyXEL Device from the ISP). It is measured in decibels. The higher the number the more signal and less noise there is.
WAN IP Address	This is the current IP address of the ZyXEL Device in the WAN. Click this to go to the screen where you can change it.
Default Gateway	This is the IP address of the default gateway, if applicable.
First DNS Secondary DNS Tertiary DNS	This is the IP address of your primary/second/third DNS server.
Local Network	
Ethernet LAN1 LAN2 LAN3 LAN4	This displays the link speed and duplex mode of the LAN port(s) in use.
Modem IP Address	This is the current IP address of the ZyXEL Device in the LAN. Click this to go to the screen where you can change it.
Modem Subnet Mask	This is the current subnet mask in the LAN.

Table 4 Status Screen

LABEL	DESCRIPTION
DHCP	This field displays what DHCP services the ZyXEL Device is providing to the LAN. Choices are: **Server** - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The ZyXEL Device is not providing any DHCP services to the LAN. Click this to go to the screen where you can change it.
DHCP Range	This is the IP address range that the ZyXEL Device is assigning to other computers in the LAN when it acts as a DHCP server.
Firewall	This displays the level of the ZyXEL Device's firewall.
Wireless Status	This displays the maximum transmission rate when WLAN is enabled.
SSID	This is the descriptive name used to identify the ZyXEL Device in a wireless LAN. Click this to go to the screen where you can change it.
Channel	This is the channel number used by the ZyXEL Device now.
Security	This displays the type of security mode the ZyXEL Device is using in the wireless LAN.
Secuirity Key	This displays the Pre-Shared Key of **WPA(2)-PSK** security mode.
WPS	This displays the status of WPS (Wi-Fi Protected Setup). Click this to go to the screen where you can change it.
More Information	
DHCP Client List	Click this link to view current DHCP client information. See Section 6.4 on page 118.
AnyIP Table	Click this link to view a list of IP addresses and MAC addresses of computers, which are not in the same subnet as the ZyXEL Device. See Section 3.3 on page 43.
Wireless Clients	Click this link to display the MAC address(es) of the wireless stations that are currently associating with the ZyXEL Device. See Section 3.4 on page 43.
Packet Statistics	Click this link to view port status and packet specific statistics. See Section 3.6 on page 45.

3.2.1 Reset to Factory Defaults

There are two methods of resetting to factory defaults.

1 In the GUI go to **Maintenance** > **Update/Reboot** > **Configuration**. Click the **Reset** button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults.

2 If you forgot your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory default configuration file. This means that you will lose all configurations that you had previously and the password will reset to “broadband1”.

3.2.1.1 Using the RESET Button

1 Make sure that the **Power** LED is on (not blinking).

2 To set the device back to the factory default settings, press the **RESET** button for 5 seconds or until the **Power** LED begins to blink. Do not turn off the device while the reset is in progress! When the **Power** LED stops blinking and lights green, the defaults have been restored and the device restarts.

3.2.2 Setting Up Remote Management for HTTP and Telnet

To enable Remote Management from the WAN for web access you have two options: create a dynamic firewall rule or manually create a firewall rule. The dynamic firewall rule is the simplest but unlike the manual firewall rule option it does not allow you to specify the source IP address(es) for WAN access.

3.2.2.1 Dynamic WWW rule

1 Click **Advanced** > **Remote MGMT** > **WWW** and set **Access Status** to **ALL** (or **LAN & WAN** or **WLAN & WAN**).

Note: IMPORTANT! If you choose WAN it will ONLY allow access from the WAN.

2 Next click on the option **Create a dynamic firewall rule** to permit WAN access and click the **Apply** button.

To disable WAN remote management for Web, simply reverse the above. Be careful to set the **Access Status** to either or both **LAN** and **WLAN**.

Note: It is recommended if you are allowing WAN access even temporarily to change the default password (in **Maintenance** > **System** > **General**).

3.2.2.2 Manual WWW Rule

1 Click **Advanced** > **Remote MGMT** > **WWW** and set **Access Status** to **ALL** (or **LAN & WAN** or **WLAN & WAN**).

Note: IMPORTANT! If you choose WAN it will ONLY allow access from the WAN.

2 Next click on the Firewall link in Note3 of the screen. For WAN access: If you want to specify the source IP address for remote management, click on the Firewall link. This will then redirect you to the main Firewall screen (**Security** >**Firewall** > **General**).

3 Here you will choose the **Custom** option (please note that the Custom option will inherit the default firewall behaviour of the firewall option that was specified previously (**High** or **Medium**, BUT NOT for **Low** as it blocks WAN to LAN access but this can easily be changed).

4 Next go to the **Rules** tab and in **Packet direction** choose **WAN to WAN/Router**. Click the **Add** button.

5 In the Edit rule page that appears you may want to change the source address from **Any**. Otherwise in **Service** > **selected services** remove **Any(TCP)** and **Any(UDP)** and move **HTTP(TCP:80)** from available services to **selected services**. Now click on the **Apply** button.

Use this screen to specify how to connect to the ZyXEL Device from a web browser, such as Internet Explorer.

To enable Remote Management from the WAN for Telnet access:

1 Go to **Advanced** > **Remote MGMT** > **Telnet** and set **Access Status** to **ALL** (or **WAN & LAN** or **WAN & WLAN**).

Note: IMPORTANT! If you choose WAN it will ONLY allow access from the WAN.

2 Next click on the Firewall link in Note3 of the screen. For WAN access: If you want to specify the source IP address for remote management, click on the Firewall link. This will then redirect you to the main Firewall screen (**Security** >**Firewall** > **General**).

3 Here you will choose the **Custom** option (please note that the Custom option will inherit the default firewall behaviour of the firewall option that was specified previously (**High** or **Medium**, BUT NOT for **Low** as it blocks WAN to LAN access but this can easily be changed).

4 Next go to the **Rules** tab and in **Packet direction** choose **WAN to WAN/Router**. Click the **Add** button.

5 In the Edit rule page that appears you may want to change the source address from **Any**. Otherwise in **Service** > **selected services** remove **Any(TCP)** and **Any(UDP)** and move **Telnet(TCP:23)** from available services to selected services. Now click on the **Apply** button.

Note: it is recommended if you are allowing WAN access even temporarily to change the default password (in **Maintenance** > **System** > **General**).

To remove Telnet remote management:

1 Go to **Advanced** > **Remote MGMT** > **Telnet** and set **Access Status** to **LAN**, **WLAN**, **WLAN & LAN** or **Disabled**.

2 Next go to **Security** > **Firewall** > **General**. There will be a **Rules** tab if **Custom** is specified as the firewall option.

3 In **Packet direction** choose **WAN to WAN/Router**.

4 Untick the Active tick box for your remote management rule and click the **Apply** button.

Note: it is recommended if you are allowing WAN access even temporarily to change the default password (in Maintenance > System > General). In the New Password box, type in a new password (up to 30 characters). Retype it in the Retype to confirm box. Then click Apply to save your changes. Use the new password to login.

3.3 DHCP Client List

See Section 6.4 on page 118 for information on this screen.

3.4 Wireless Clients

Use this screen to view the wireless stations that are currently associated to the ZyXEL Device. Click **Status > Wireless Clients** to access this screen.

Figure 8 Wireless Clients

The following table describes the labels in this screen.

Table 5 WLAN Status

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC (Media Access Control) address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the ZyXEL Device.
Refresh	Click this to reload this screen.

3.5 Any IP Table

Click **Status > AnyIP Table** to access this screen. Use this screen to view the IP address and MAC address of each computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.

Figure 9 Any IP Table

Each field is described in the following table.

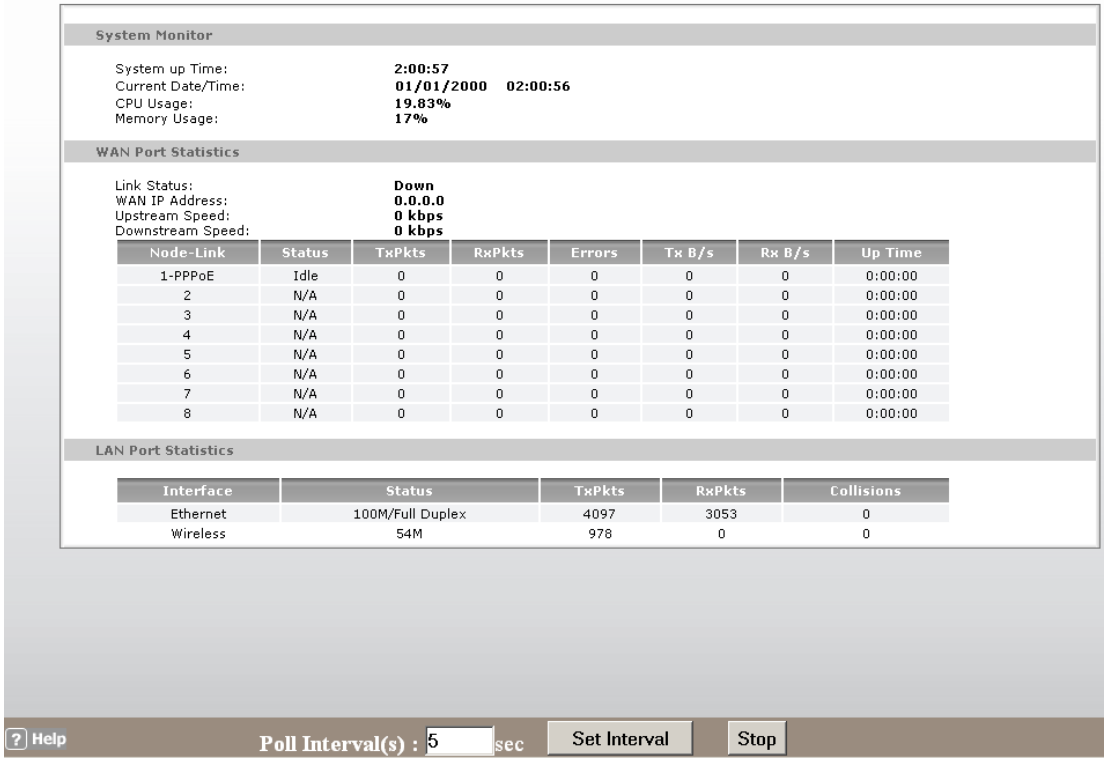
Table 6 Any IP Table

LABEL	DESCRIPTION
#	This field is a sequential value. It is not associated with a specific entry.
IP Address	This field displays the IP address of each computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.
MAC Address	This field displays the MAC address of the computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.
Refresh	Click this to update this screen.

3.6 Packet Statistics

Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable. Click **Status > Packet Statistics** to access this screen.

Figure 10 Packet Statistics


System Monitor
System up Time: 2:00:57
Current Date/Time: 01/01/2000 02:00:56
CPU Usage: 19.83%
Memory Usage: 17%
WAN Port Statistics
Link Status: Down
WAN IP Address: 0.0.0.0
Upstream Speed: 0 kbps
Downstream Speed: 0 kbps
Node-Link Status TxPkts RxPkts Errors Tx B/s Rx B/s Up Time
1-PPPoE Idle 0 0 0 0 0 0:00:00
2 N/A 0 0 0 0 0 0:00:00
3 N/A 0 0 0 0 0 0:00:00
4 N/A 0 0 0 0 0 0:00:00
5 N/A 0 0 0 0 0 0:00:00
6 N/A 0 0 0 0 0 0:00:00
7 N/A 0 0 0 0 0 0:00:00
8 N/A 0 0 0 0 0 0:00:00
LAN Port Statistics
Interface Status TxPkts RxPkts Collisions
Ethernet 100M/Full Duplex 4097 3053 0
Wireless 54M 978 0 0
Help
Poll Interval(s) : 5 sec
Set Interval
Stop

The following table describes the fields in this screen.

Table 7 Packet Statistics

LABEL	DESCRIPTION
System Monitor	
System up Time	This is the elapsed time the system has been up.
Current Date/ Time	This field displays your ZyXEL Device's present date and time.
CPU Usage	This field specifies the percentage of CPU utilization.
Memory Usage	This field specifies the percentage of memory utilization.
WAN Port Statistics	
Link Status	This is the status of your WAN link.
WAN IP Address	This is the IP address of the ZyXEL Device's WAN port.
Upstream Speed	This is the upstream speed of your ZyXEL Device.
Downstream Speed	This is the downstream speed of your ZyXEL Device.

Table 7 Packet Statistics (continued)

LABEL	DESCRIPTION
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
Status	This field displays **Down** (line is down), **Up** (line is up or connected) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
LAN Port Statistics	
Interface	This field displays either **Ethernet** (LAN ports) or **Wireless** (WLAN port).
Status	For the LAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN port, it displays the transmission rate when WLAN is enabled or **N/A** when WLAN is disabled.
TxPkts	This field displays the number of packets transmitted on this interface.
RxPkts	This field displays the number of packets received on this interface.
Collisions	This is the number of collisions on this interfaces.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this to apply the new poll interval you entered in the **Poll Interval** field above.
Stop	Click this to halt the refreshing of the system statistics.

4

Tutorials

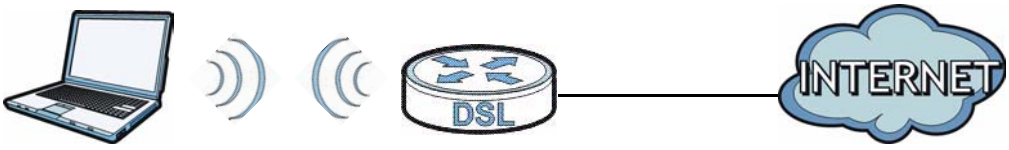
4.1 Overview

This chapter shows you how to use the ZyXEL Device's various features.

- Setting Up a Secure Wireless Network, see page 47
- Setting Up Multiple Wireless Groups, see page 55
- Configuring the MAC Address Filter, see page 59
- Access the ZyXEL Device Using DDNS, see page 61
- Configuring Static Route for Routing to Another Network, see page 65
- Multiple Public and Private IP Address Mappings, see page 67
- ATM QoS and QoS Overview, see page 71
- Setting Up NAT Port Forwarding, see page 82

4.2 Setting Up a Secure Wireless Network

Thomas wants to set up a wireless network so that he can use his notebook to access the Internet. In this wireless network, the ZyXEL Device serves as an access point (AP), and the notebook is the wireless client. The wireless client can access the Internet through the AP.



Thomas has to configure the wireless network settings on the ZyXEL Device. Then he can set up a wireless network using WPS (Section 4.2.2 on page 49) or manual configuration (Section 4.2.3 on page 54).

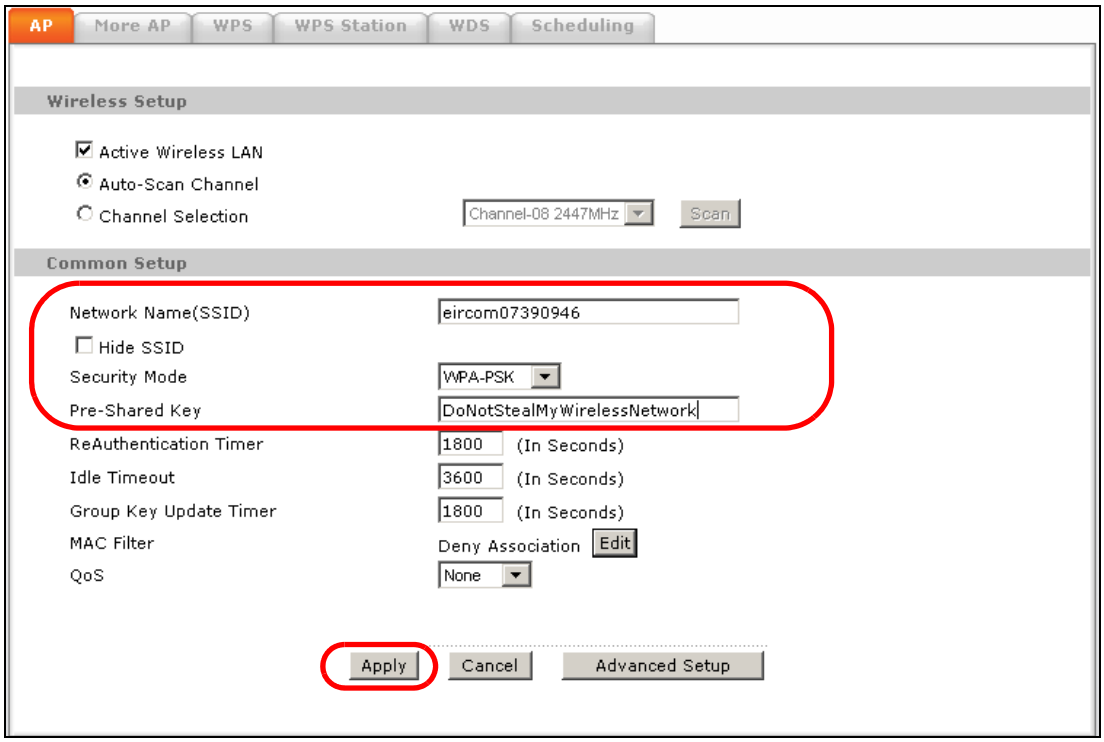
4.2.1 Configuring the Wireless Network Settings

This example uses the following parameters to set up a wireless network.

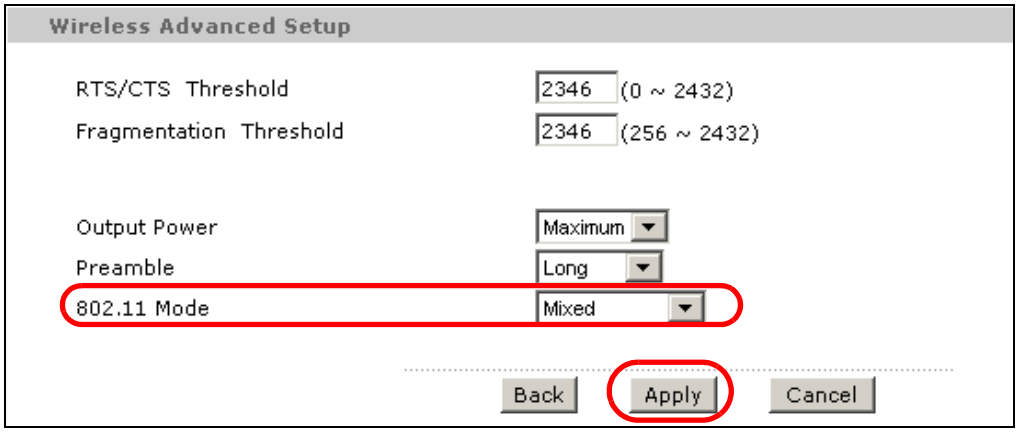
SSID	eircom07390946
Security Mode	WPA-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork
802.11 Mode	Mixed

1 Click **Network** > **Wireless LAN** to open the **AP** screen. Configure the screen using the provided parameters (see page 48). Click **Apply**.

Note: To see the default SSID, check the sticker on the rear panel of your ZyXEL Device. To see the current SSID, go to the **Status** screen.



2 Click the **Advanced Setup** button and select **Mixed** in the **802.11 Mode** field. Click **Apply**.



Thomas can now use the WPS feature to establish a wireless connection between his notebook and the ZyXEL Device (see Section 4.2.2 on page 49). He can also use the notebook's wireless client to search for the ZyXEL Device (see Section 4.2.3 on page 54).

4.2.2 Using WPS

This section shows you how to set up a wireless network using WPS. It uses the ZyXEL Device as the AP and ZyXEL NWD210N as the wireless client which connects to the notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCMCIA card).

There are two WPS methods to set up the wireless client settings:

- **Push Button Configuration (PBC)** - simply press a button. This is the easier of the two methods.
- **PIN Configuration** - configure a Personal Identification Number (PIN) on the ZyXEL Device. A wireless client must also use the same PIN in order to download the wireless network settings from the ZyXEL Device.

Push Button Configuration (PBC)

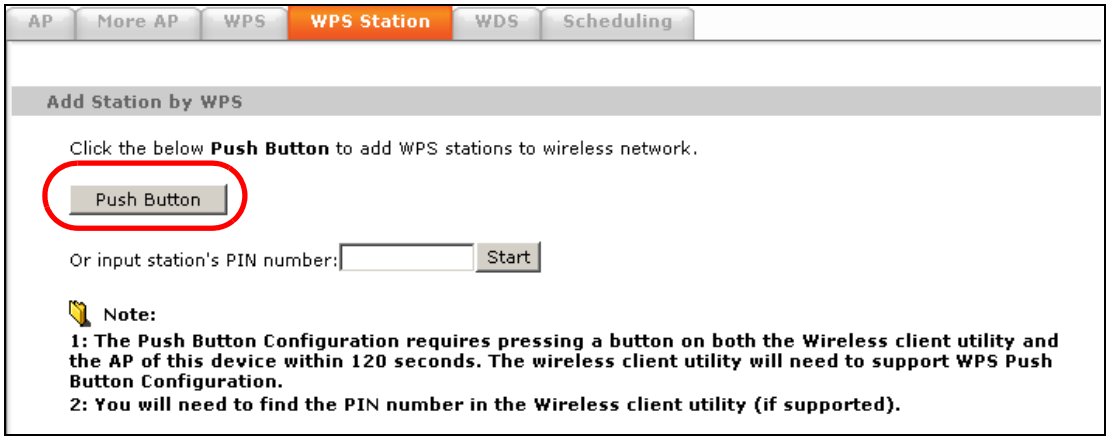
1 Make sure that your ZyXEL Device is turned on and your notebook is within the cover range of the wireless signal.

2 Make sure that you have installed the wireless client driver and utility in your notebook.

3 Press the WiFi or WPS button on your notebook within range of the ZyXEL Device.

4 The wireless LAN of the ZyXEL Device is enabled by default, so the LED lights green. If not, press the **WIFI** button for 5 to 6 seconds and release it when the LED turns green. The wireless LAN is on. Then press the WIFI button for 1 to 2 seconds and release it when the LED is blinking orange.

5 Alternatively, you may log into ZyXEL Device's web configurator and click the **Push Button** in the **Network** > **Wireless LAN** > **WPS Station** screen.

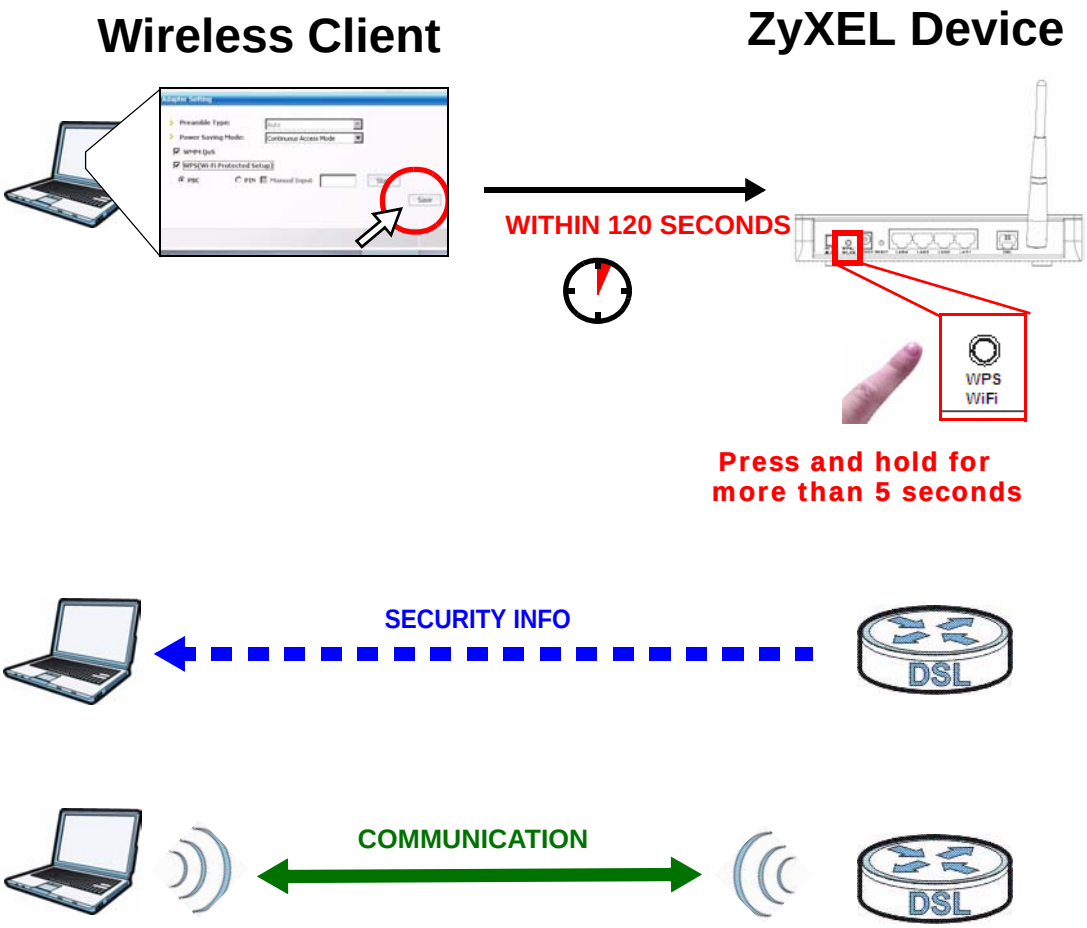

AP
More AP
WPS
WPS Station
WDS
Scheduling
Add Station by WPS
Click the below Push Button to add WPS stations to wireless network.
Push Button
Or input station's PIN number:
Start
Note:
1: The Push Button Configuration requires pressing a button on both the Wireless client utility and the AP of this device within 120 seconds. The wireless client utility will need to support WPS Push Button Configuration.
2: You will need to find the PIN number in the Wireless client utility (if supported).

Note: Your ZyXEL Device has a WIFI button located on its rear panel as well as a WPS button in its configuration utility. Both buttons have exactly the same function: you can use one or the other.

Note: It doesn't matter which button is pressed first. You must press the second button within 120 seconds of pressing the first one.

6 When the ZyXEL Device is sending the configuration settings to the wireless client, the WiFi LED blinks orange. This may take up to two minutes. Then the WiFi LED becomes green when the wireless client is able to communicate with the ZyXEL Device securely. (You can refer to Section 1.7.2 on page 28 for more information on activating WPS.)

The following figure shows you an example of how to set up a wireless network and its security by pressing a button on both ZyXEL Device and wireless client.

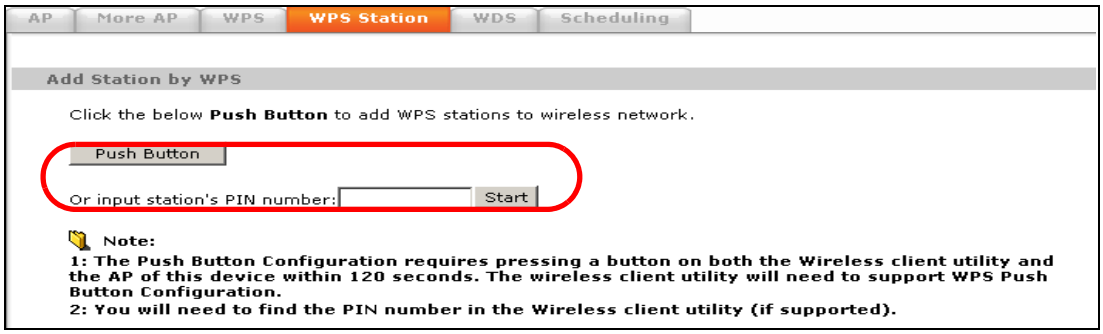


PIN Configuration

When you use the PIN configuration method, you need to use both the ZyXEL Device's web configurator and the wireless client's utility.

1 Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.

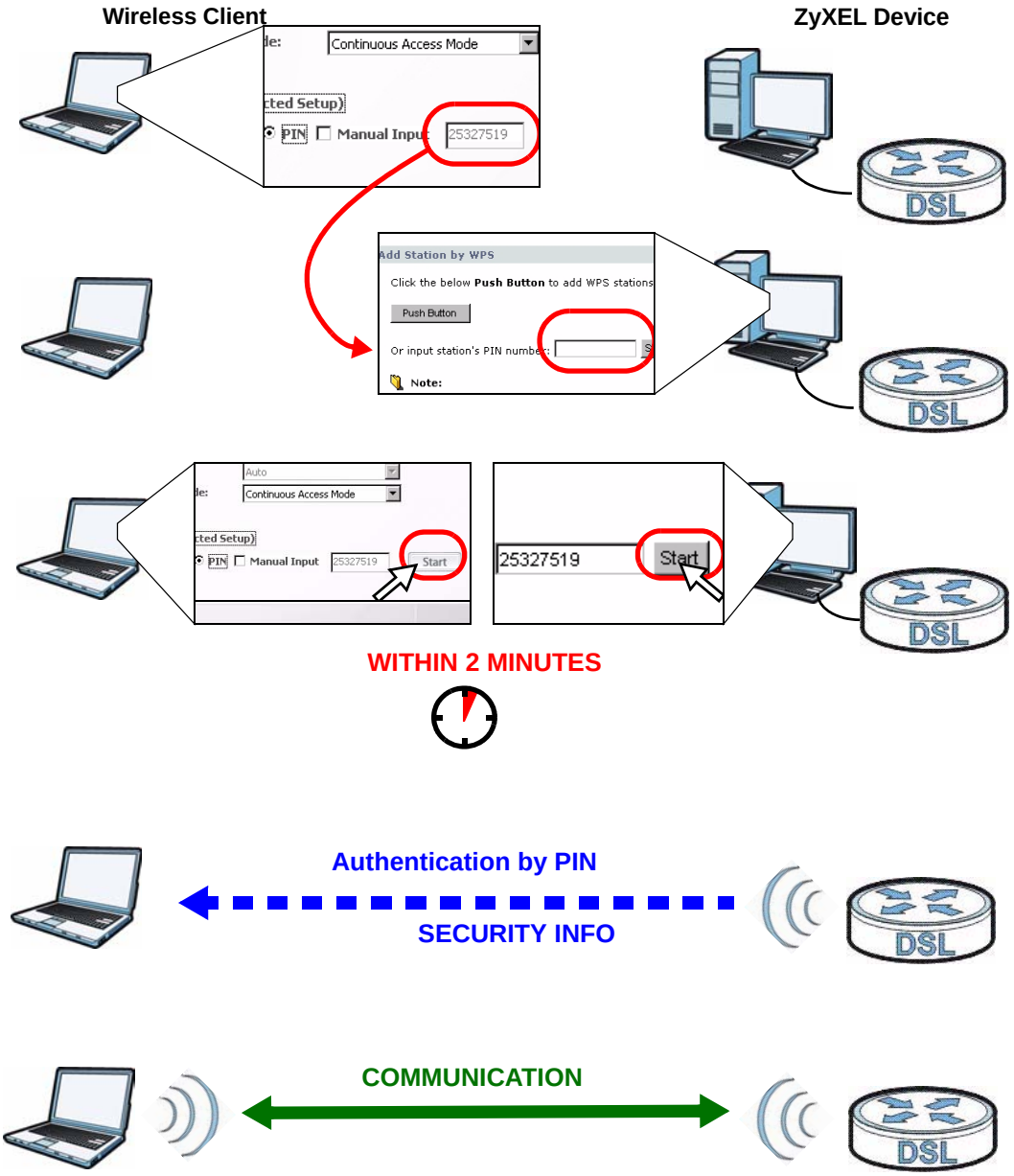
2 Enter the PIN number in the **PIN** field in the **Network** > **Wireless LAN** > **WPS Station** screen on the ZyXEL Device.


AP
More AP
WPS
WPS Station
WDS
Scheduling
Add Station by WPS
Click the below Push Button to add WPS stations to wireless network.
Push Button
Or input station's PIN number:
Start
Note:
1: The Push Button Configuration requires pressing a button on both the Wireless client utility and the AP of this device within 120 seconds. The wireless client utility will need to support WPS Push Button Configuration.
2: You will need to find the PIN number in the Wireless client utility (if supported).

3 Click the **Start** buttons (or the button next to the PIN field) on both the wireless client utility screen and the ZyXEL Device's **WPS Station** screen within two minutes.

The ZyXEL Device authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the ZyXEL Device securely.

The following figure shows you how to set up a wireless network and its security on a ZyXEL Device and a wireless client by using PIN method.



4.2.3 Without WPS

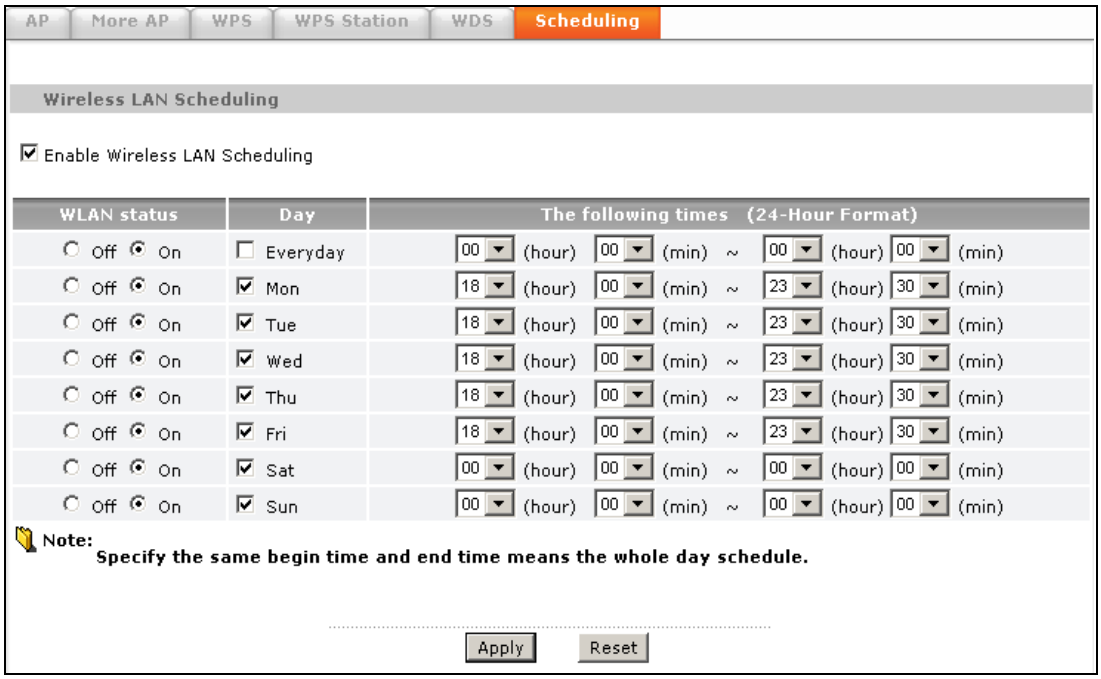
Use the wireless adapter's utility installed on the notebook to search for the "Example" SSID. Then enter the "DoNotStealMyWirelessNetwork" pre-shared key to establish an wireless Internet connection.

Note: The ZyXEL Device supports IEEE 802.11b and IEEE 802.11g wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

4.2.4 Setting Up Wireless Network Scheduling

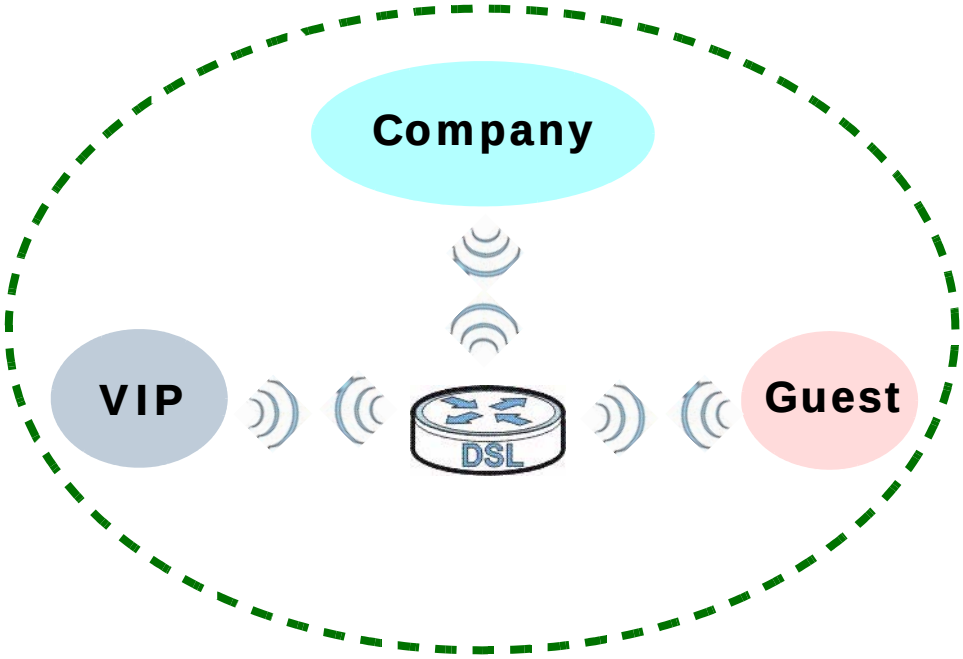
Thomas mostly uses his notebook to access the Internet on weekends; occasionally he uses it at night on weekdays. Here is how Thomas can set up a schedule to turn on the wireless network at specific time and days.

1 Click **Network** > **Wireless LAN** > **Scheduling** to open the following screen and configure as follows. Turn on the wireless network from Mondays to Fridays between 18:00 and 23:30. Turn on the wireless network all day on Saturdays and Sundays. Click **Apply**.



4.3 Setting Up Multiple Wireless Groups

Company A wants to create different wireless network groups for different types of users as shown in the following figure. Each group has its own SSID, security mode and QoS control.

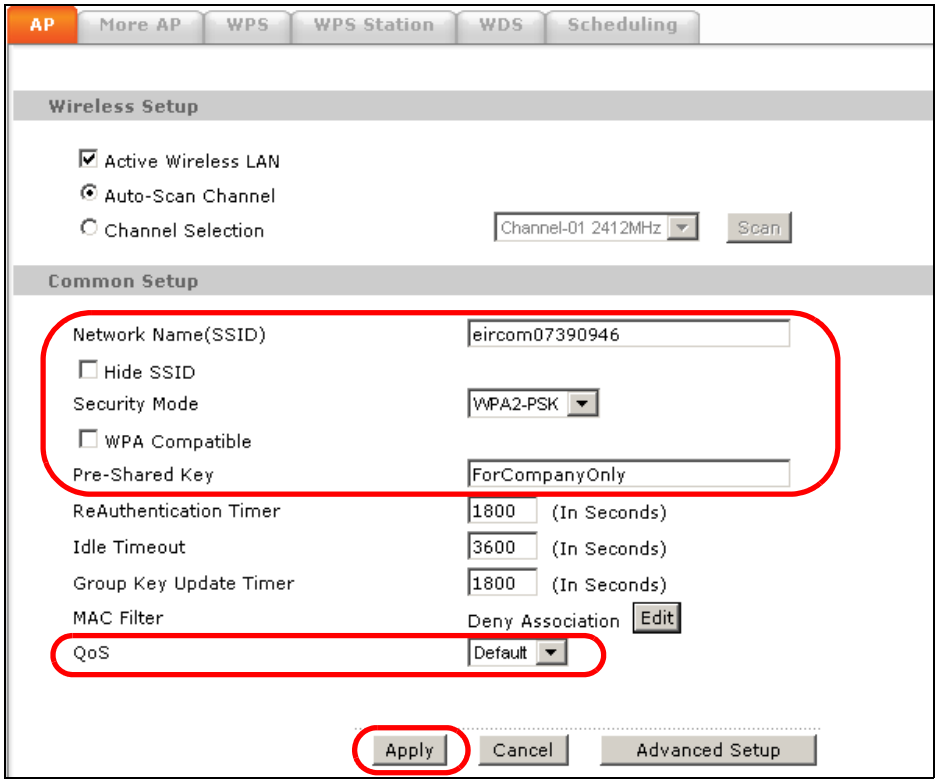


- Employees in Company A will use a general eircom07390946 wireless network group.
- Higher management level and important visitors will use the VIP group, which has the highest QoS control.
- Visiting guests will use the Guest group, which has a lower security mode and QoS control.

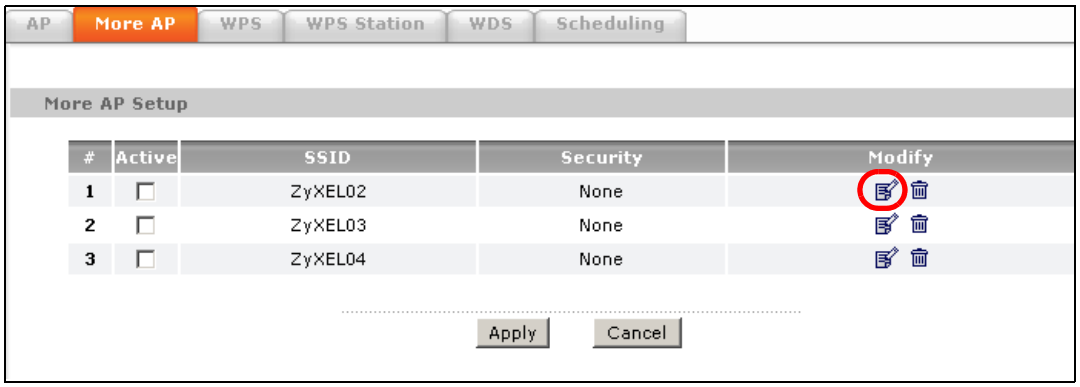
Company A will use the following parameters to set up the wireless network groups.

	COMPANY	VIP	GUEST
SSID	eircom07390946	VIP	Guest
Security Mode	WPA2-PSK	WPA2-PSK	Static WEP
Pre-Shared Key	ForCompanyOnly	ForVIPOnly	Guest
QoS	Default	Highest	Low

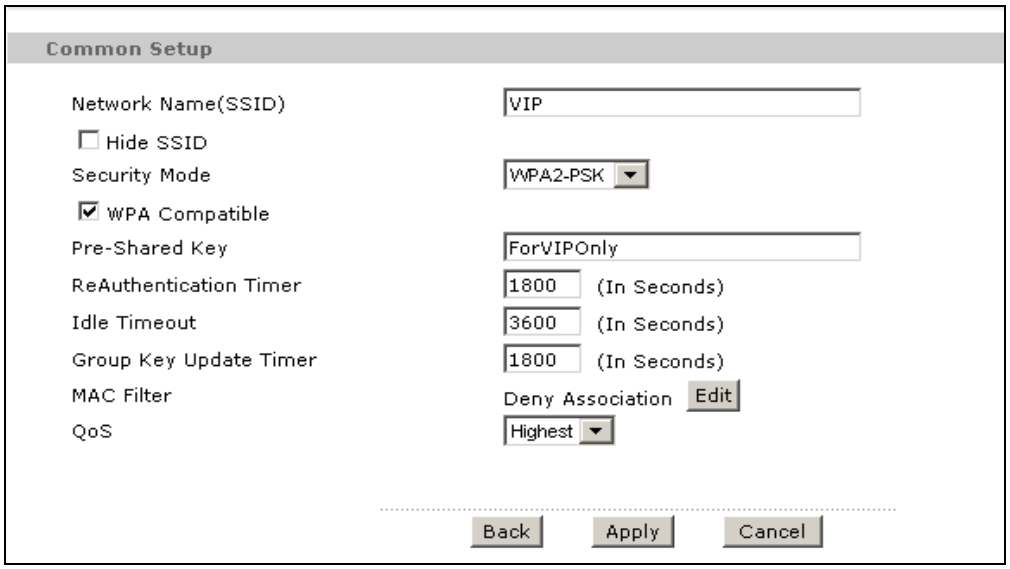
1 Click **Network** > **Wireless LAN** to open the **AP** screen. Use this screen to set up the company's general wireless network group. Configure the screen using the provided parameters and click **Apply**.



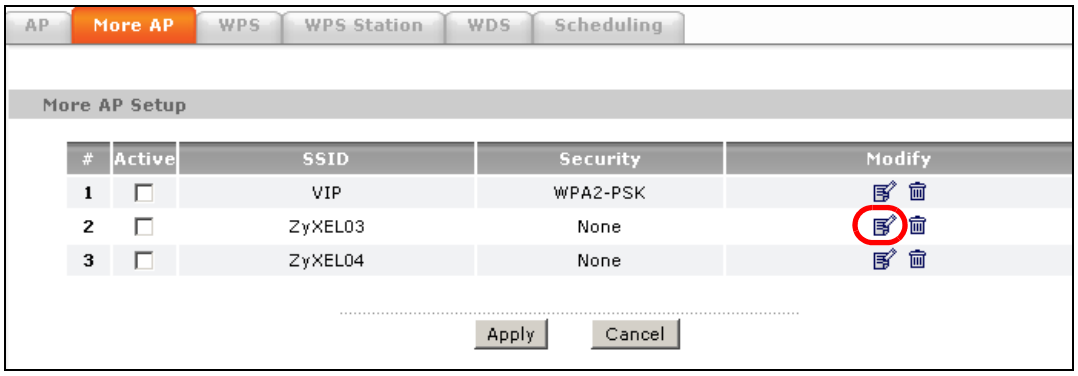
2 Click **Network** > **Wireless LAN** > **More AP** to open the following screen. Click the **Edit** icon to configure the second wireless network group.



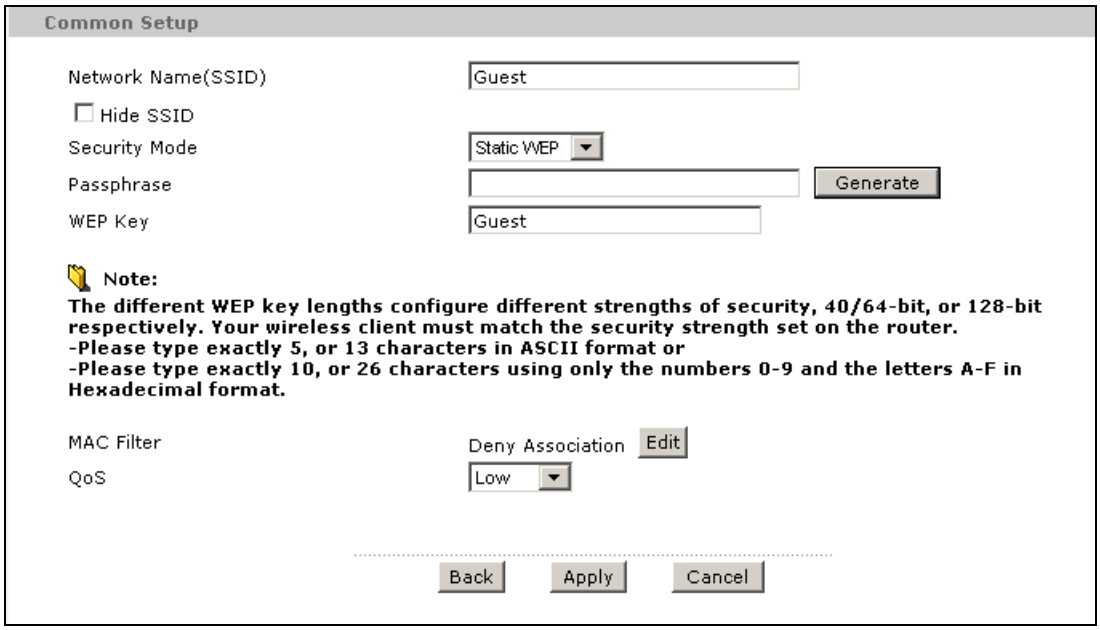
3 Configure the screen using the provided parameters and click **Apply**.



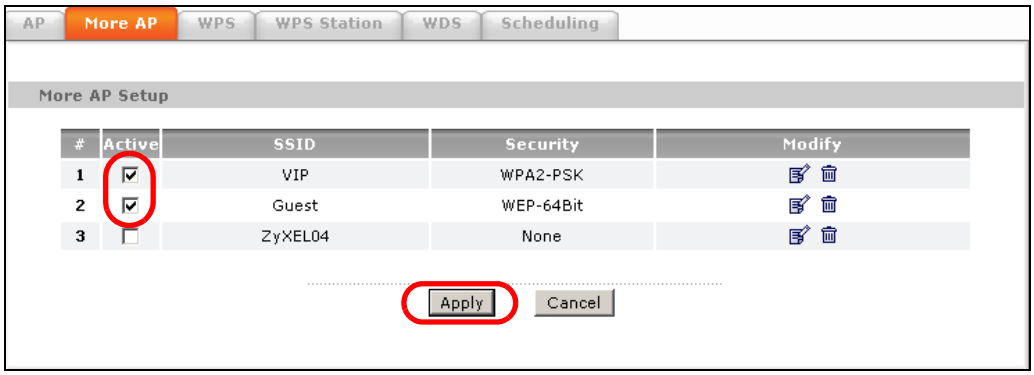
4 In the **More AP** screen, click the **Edit** icon to configure the third wireless network group.



5 Configure the screen using the provided parameters and click **Apply**.



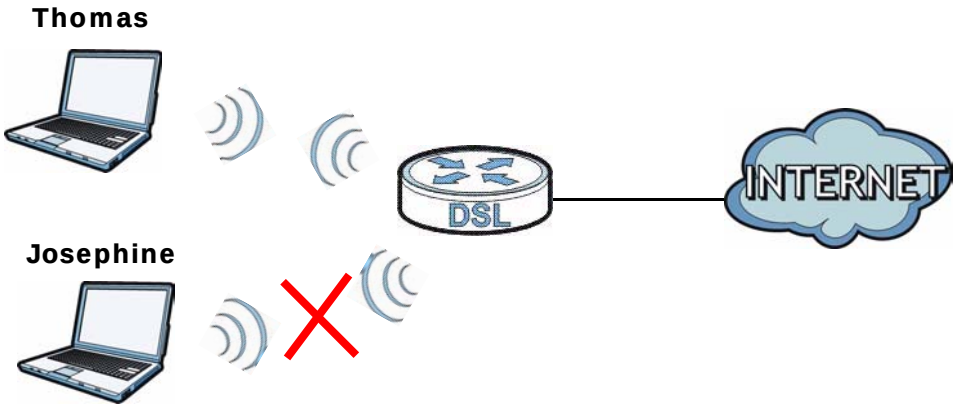
6 Activate the wireless network groups and click **Apply**.



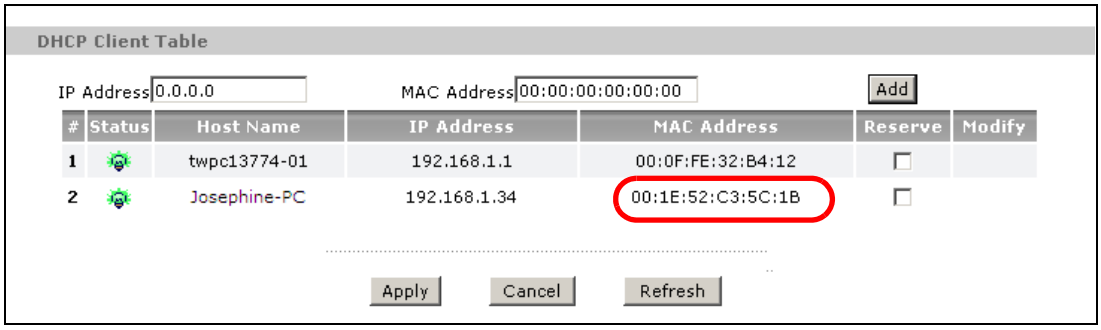
4.4 Configuring the MAC Address Filter

Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

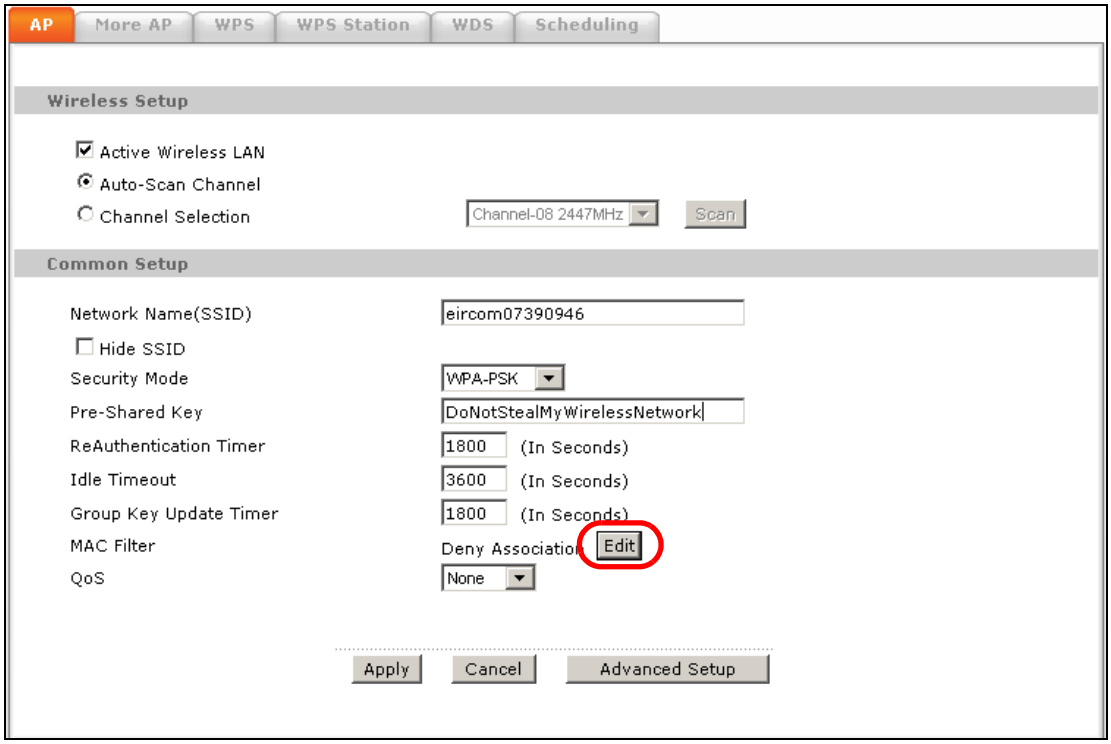
Josephine's computer connects wirelessly to the Internet through the ZyXEL Device. Thomas can deny access to the wireless network using the MAC address of Josephine's computer.



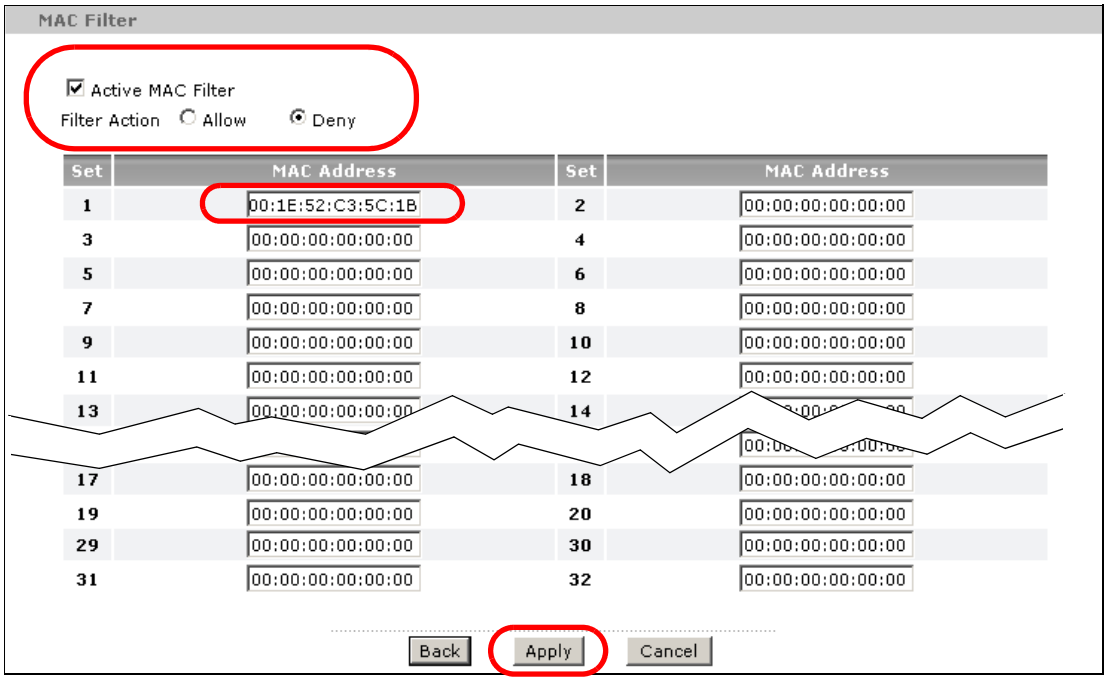
1 Click **Network** > **Local Network (LAN)** > **Client List** to open the following screen. Look for the MAC address of Josephine's computer.



2 Click **Network** > **Wireless LAN** to open the **AP** screen. Click the **Edit** button in the **MAC Filter** field.



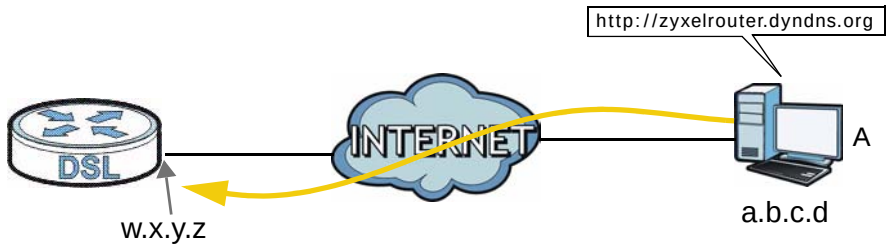
3 Select **Active MAC Filter** and **Deny Filter Action**. Enter the MAC address you found in the **Client List** screen. Click **Apply**.



Josephine will no longer be able to access the Internet through the ZyXEL Device.

4.5 Access the ZyXEL Device Using DDNS

If you connect your ZyXEL Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The ZyXEL Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the ZyXEL Device using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial shows you how to:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your ZyXEL Device
- Adding a Firewall Rule for Remote Management
- Testing the DDNS Setting

Note: If you have a private WAN IP address, then you cannot use DDNS.

4.5.1 Registering a DDNS Account on www.dyndns.org

1. Open a browser and type **http://www.dyndns.org**.
2. Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.
3. Log into www.dyndns.org using your account.
4. Add a new DDNS host name. This tutorial uses the following settings as an example.
   - Hostname: **zyxelrouter.dyndns.org**
   - Service Type: **Host with IP address**
   - IP Address: Enter the WAN IP address that your ZyXEL Device is currently using. You can find the IP address on the ZyXEL Device's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the ZyXEL Device later.

4.5.2 Configuring DDNS on Your ZyXEL Device

1 Log into the ZyXEL Device's advanced mode.

2 Configure the following settings in the **Advanced** > **Dynamic DNS** screen.

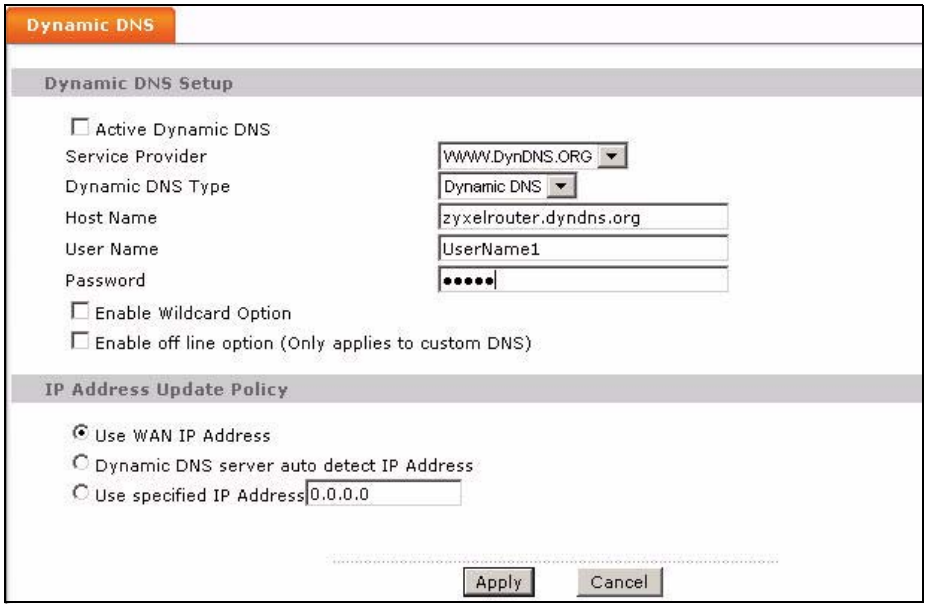
2a Select **Active Dynamic DNS**.

2b Select **Dynamic DNS** for the DDNS type.

2c Type **zyxelrouter.dyndns.org** in the **Host Name** field.

2d Enter the user name (**UserName1**) and password (**12345**).

2e Select **Use WAN IP Address** for the IP address update policy.



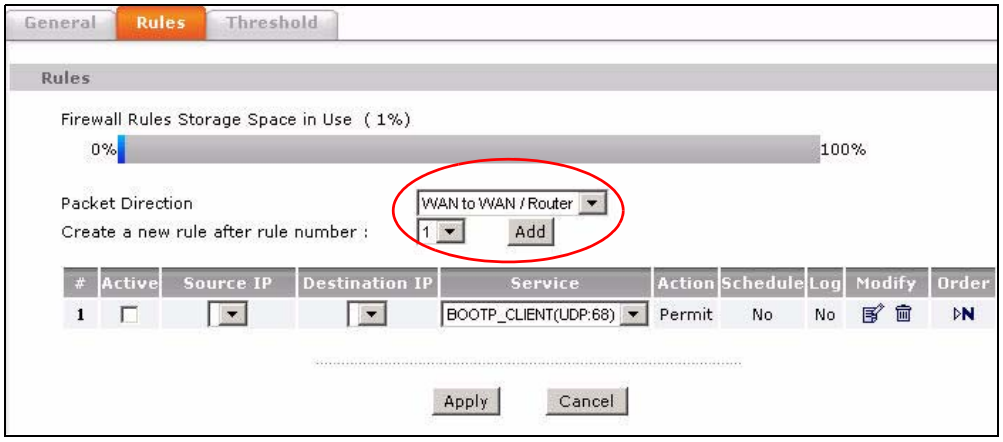
2f Click **Apply**.

4.5.3 Adding a Firewall Rule for Remote Management

By default, your ZyXEL Device firewall is enabled to secure your network from attacks. In this tutorial, you add a firewall rule that lets you manage the ZyXEL Device from the Internet.

1 Select **Custom** from the **General** screen. The **Rules** tab will appear. Click the tab to go to **Rules** screen.

2 Select **WAN to WAN / Router** and select the number of the last rule that has been configured on this screen. Click **Add**.



3 The **Edit Rule** screen opens. Configure the screen using the following settings.

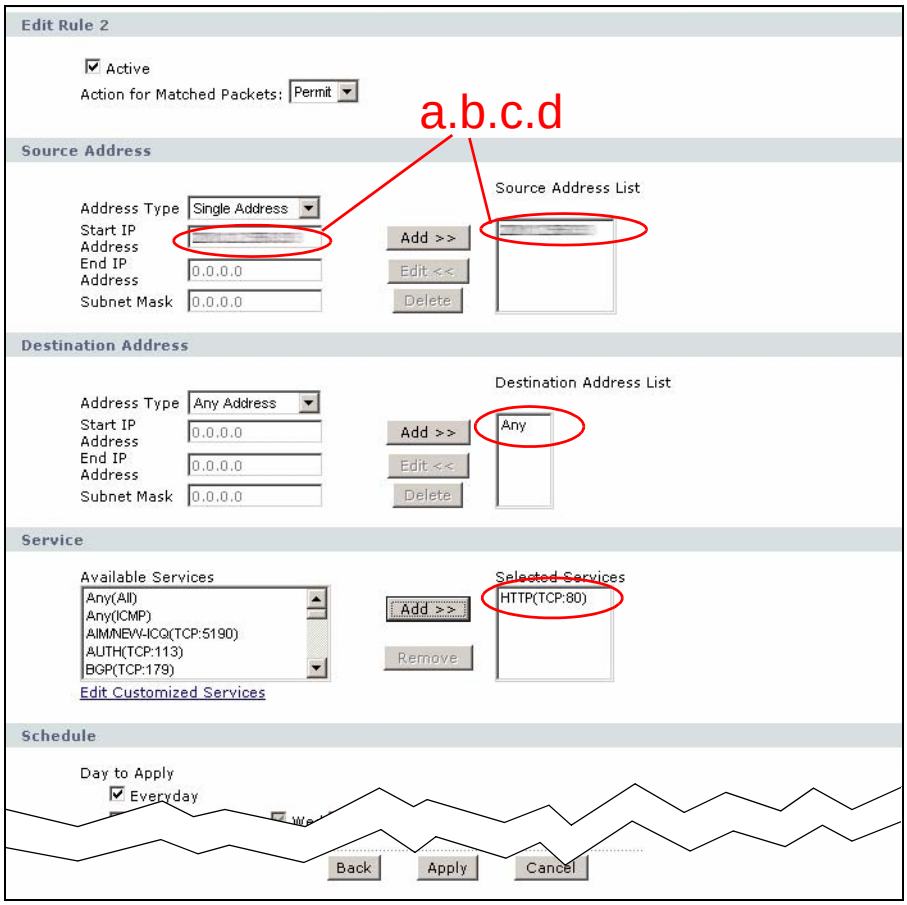
3a Select **Active**.

3b Select **Permit** for matched packets.

3c In the **Source Address** section, select **Single Address** and enter the IP address of the computer that you allow to access the ZyXEL Device from the Internet. Click **Add**. Select **Any** in the **Source Address List** and click **Delete**.

Note: If the computer gets a different IP address, this firewall rule will not work.

3d In the **Service** section, select **HTTP(TCP:80)** in the **Available Services** field and click **Add**. Select **Any(UDP)** and **Any(TCP)** and click **Remove** one-by-one to not include them.



3e Click **Apply**.

4.5.4 Testing the DDNS Setting

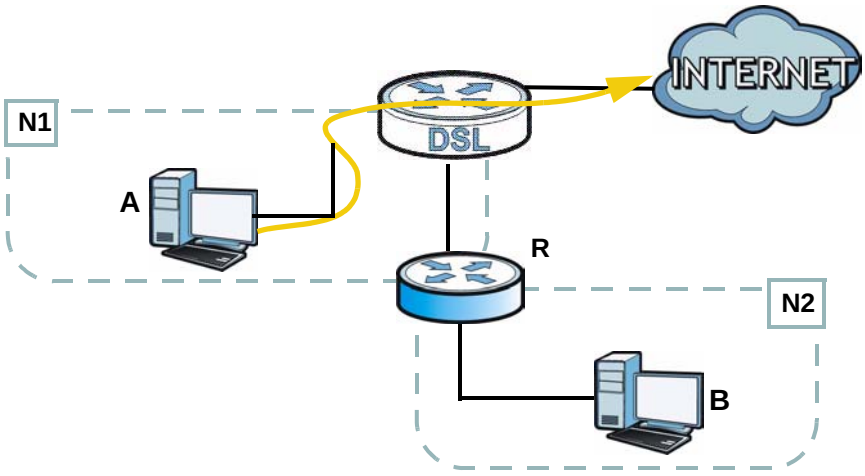
Now you should be able to access the ZyXEL Device from the Internet. To test this:

1. Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.
2. Type **http://zyxelrouter.dyndns.org** and press [Enter].
3. The ZyXEL Device's login page should appear. You can then log into the ZyXEL Device and manage it.

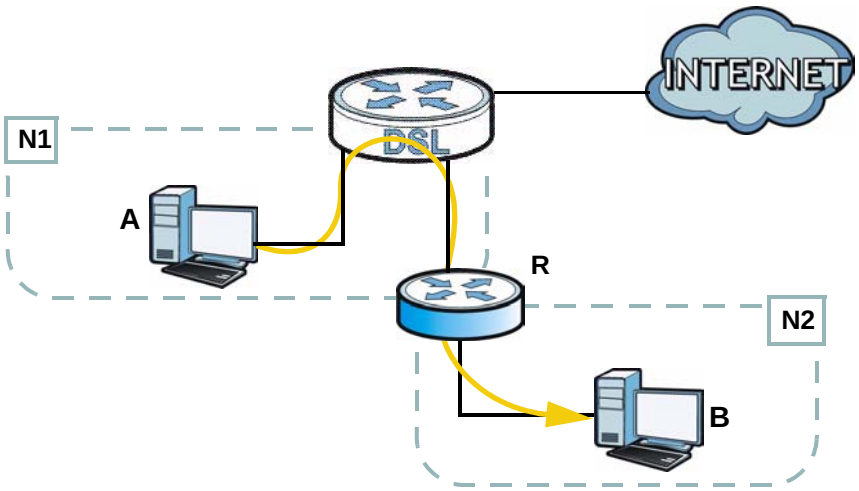
4.6 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the ZyXEL Device's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the ZyXEL Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the ZyXEL Device's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the ZyXEL Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the ZyXEL Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

Table 8 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The ZyXEL Device's WAN	172.16.1.1
The ZyXEL Device's LAN	192.168.1.1
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

1 Log into the ZyXEL Device's Web Configurator in advanced mode.

2 Click **Advanced** > **Static Route**.

3 Click **Edit** on a new rule in the **Static Route** screen.

4 Configure the **Static Route Setup** screen using the following settings:

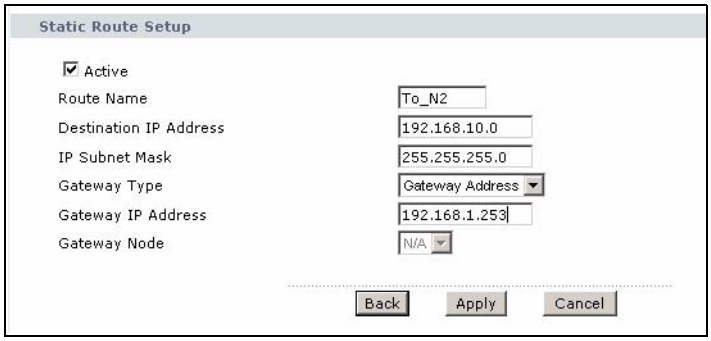
4a Select **Active**.

4b Specify a descriptive name for this routing rule.

4c Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.

4d Select **Gateway Address** for the gateway type.

4e Type **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.

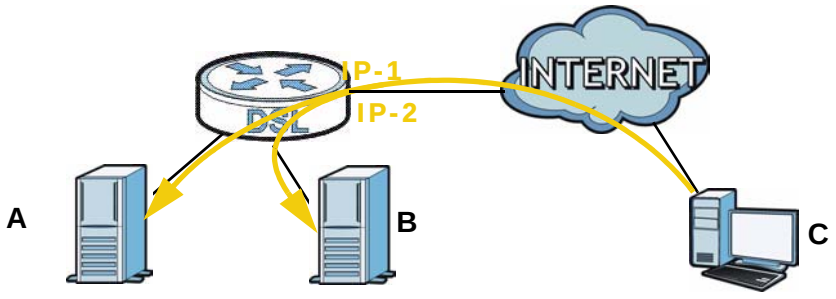


4a Click **Apply**.

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.

4.7 Multiple Public and Private IP Address Mappings

If your ISP gives you more than one static IP address for your Internet access, you can map each IP address for a specific service. This tutorial assumes you are given two static public IP addresses. You want to map them to two servers **A** and **B**.



This tutorial uses the following example settings:

Table 9 IP Settings in this Tutorial

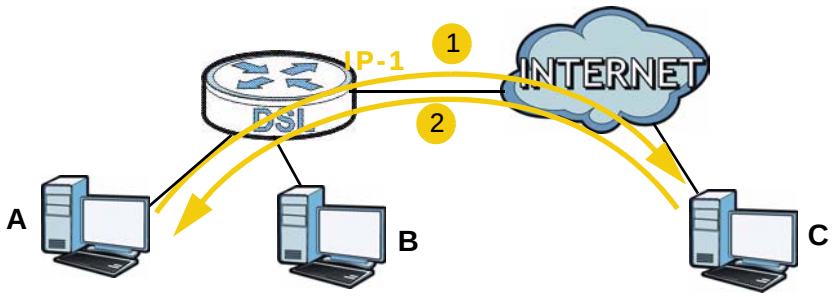
DEVICE / COMPUTER	IP ADDRESS
The ZyXEL Device's WAN	172.16.1.253 (**IP-1**) 172.16.1.254 (**IP-2**)
The ZyXEL Device's LAN	192.168.1.1
A	192.168.1.2
B	192.168.1.3
C	a.b.c.d

To do this, you can use either of the following settings:

- Full Feature NAT with many-to-many no overload mapping
- Full Feature NAT with one-to-one mapping

4.7.1 Full Feature NAT + Many-to-Many No Overload Mapping

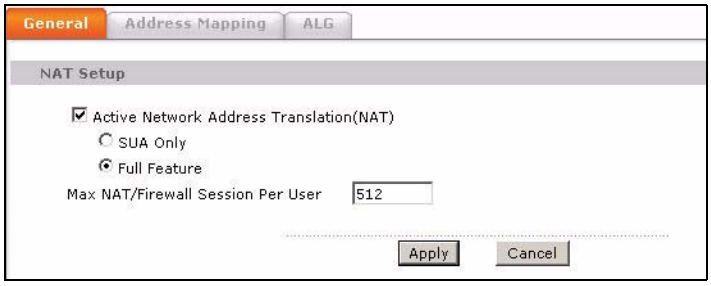
Use this setting if your applications can use random public IP addresses and the applications are initiated from the Intranet computers (**A** and **B**). For example, VoIP application. See Section 4.7.2 on page 70 if it is not.



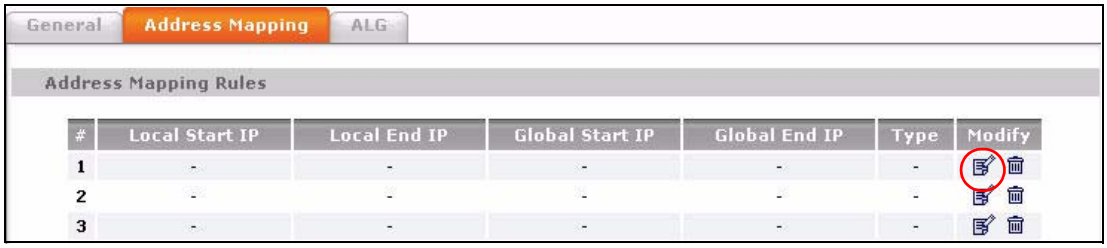
To configure this:

1 Click **Network** > **NAT**.

2 Select **Active Network Address Translation(NAT)** and **Full Feature** in the **General** screen. Click **Apply**.

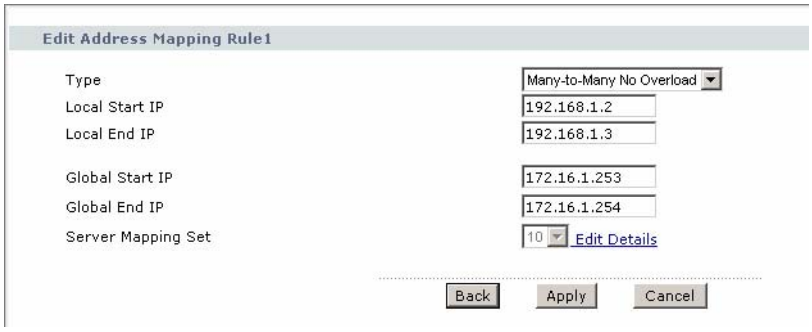


3 Click the **Address Mapping** tab, and then click the **Edit** icon on a new rule.


General
Address Mapping
ALG
Address Mapping Rules
Local Start IP Local End IP Global Start IP Global End IP Type Modify
1 - - - - -
2 - - - - -
3 - - - - -

4 Configure the rule using the following settings:

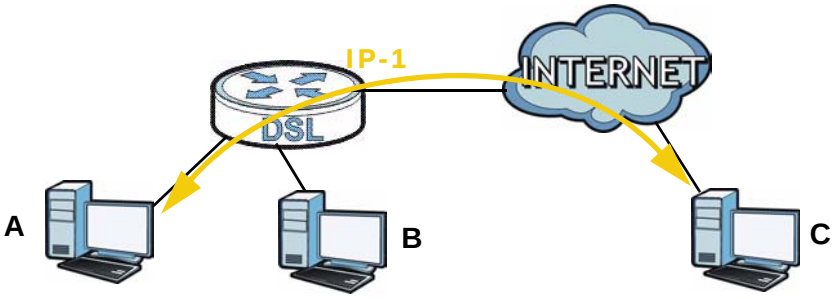
- Type: **Many-to-Many No Overload**
- Local IP addresses: **192.168.1.2** ~ **192.168.1.3**
- Global IP addresses: **172.16.1.253** ~ **172.16.1.254**



Then click **Apply**.

4.7.2 Full Feature NAT + One-to-One Mapping

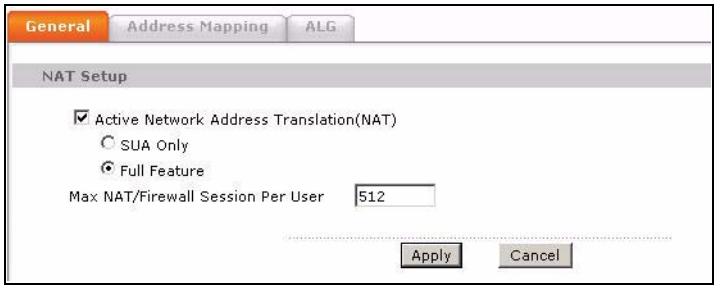
Use this setting if your applications must use fixed public IP addresses and the applications can be initiated either from the Intranet computers (**A** and **B**) or the Internet computer (**C**). For example, gaming application.



To configure this setting:

1 Click **Network** > **NAT**.

2 Select **Active Network Address Translation(NAT)** and **Full Feature** in the **General** screen. Click **Apply**.



3 Click the **Address Mapping** tab, click the **Edit** icon on a new rule.

General
Address Mapping
ALG
Address Mapping Rules
Local Start IP Local End IP Global Start IP Global End IP Type Modify
1 - - - - -
2 - - - - -
3 - - - - -

4 Configure two rules for the one-to-one mappings:

- Rule 1 (This maps the public IP address 172.16.1.253 to the private IP address 192.168.1.2)

  Type: **One-to-One**

  Local Start IP: **192.168.1.2**

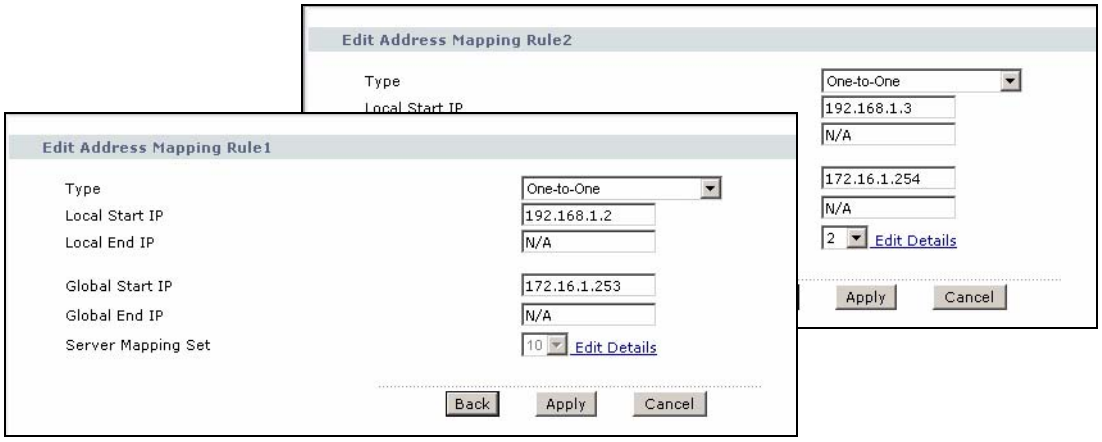
Global Start IP: **172.16.1.253**

- Rule 2 (This maps the public IP address 172.16.1.254 to the private IP address 192.168.1.3)

  Type: **One-to-One**

  Local Start IP: **192.168.1.3**

  Global Start IP: **172.16.1.254**



Click **Apply** on each of the screens.

4.8 ATM QoS and QoS Overview

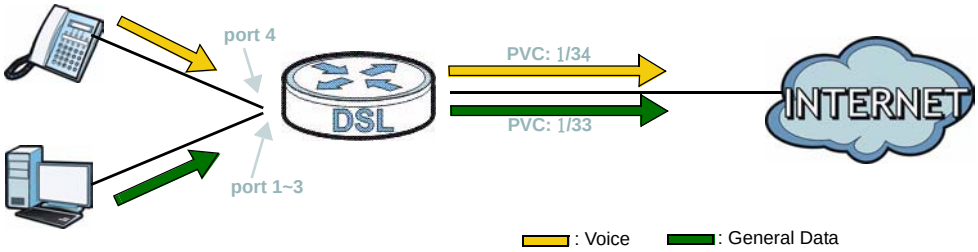
Use the **Network > Internet (WAN)** menus to create PVCs and apply **UBR**, **CBR** or **VBR** ATM QoS to them.

Use the **Advanced > QoS** menus to identify individual packets, assign each packet a priority and then queue the packet. Packets assigned with a high priority are processed more quickly than those with low priorities if there is network congestion.

4.8.1 Two PVCs with ATM QoS Scenario

This tutorial shows you how to configure two PVCs and specify an ATM QoS type for each PVC. In the following figure, the ZyXEL Device is configured to transmit two types of traffic, general data for Internet access and VoIP using SIP using 1/33 and 1/34 PVCs respectively. General data is assigned Unspecified Bit Rate

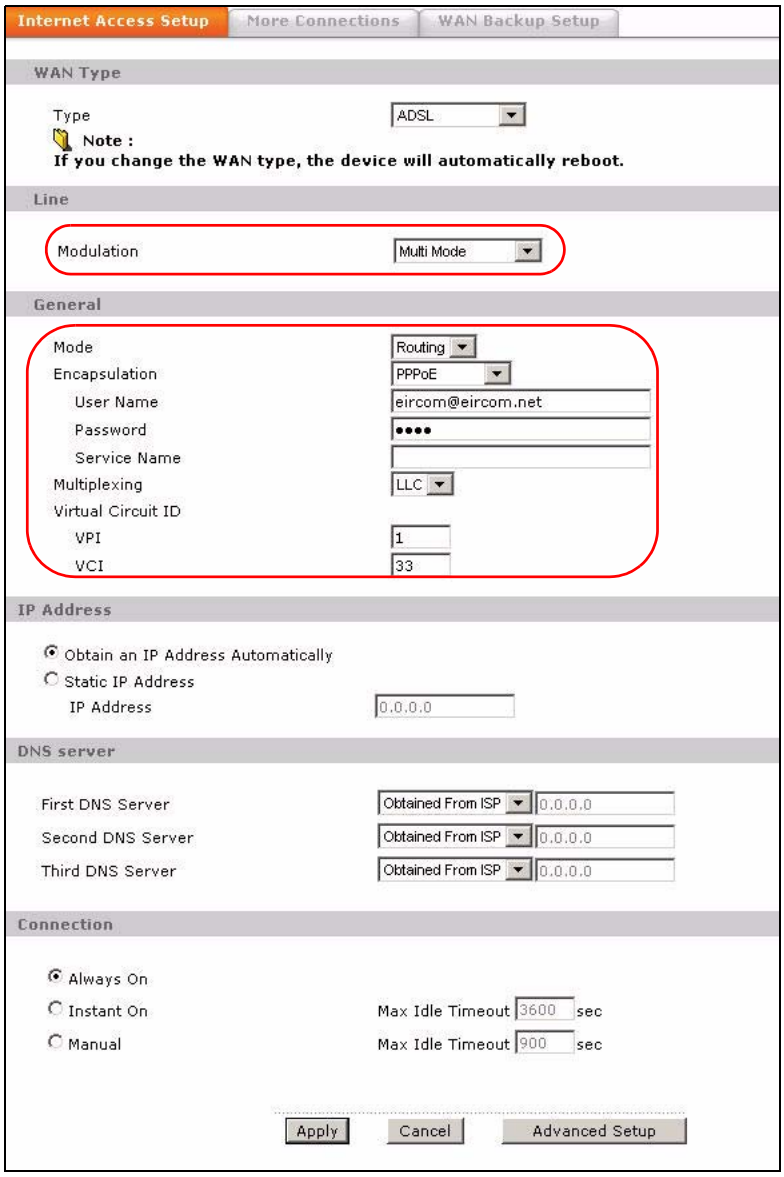
(UBR) ATM QoS while VoIP traffic is assigned Constant Bit Rate (CBR) ATM QoS as it is considered to transmit continuously.



4.8.1.1 PVC 1 for Internet Access (General Data)

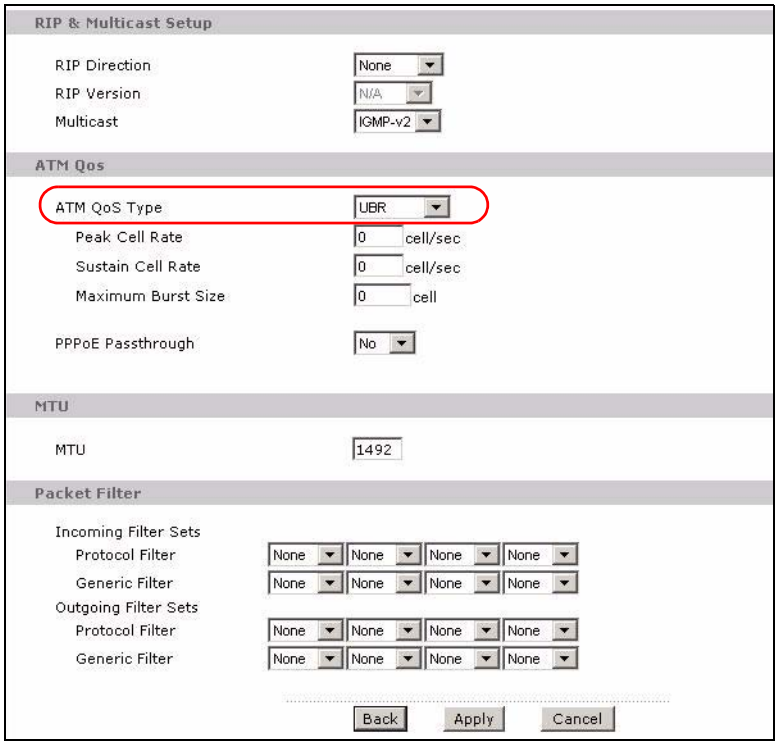
1 Click **Network** > **Internet (WAN)** > **Internet Access Setup**, configure the settings you (ISP) want to provide to the subscriber for general data transmission. This tutorial uses the following example settings:

- Line Modulation: **Multi Mode**
- Mode: **Routing**
- Encapsulation: **PPPoE**
- User Name: **eircom@eircom.net**
- Password: **1234**
- PVC: **LLC**, **1/33**
- ATM QoS: **UBR**



2 Leave the other settings as their defaults and click **Apply**.

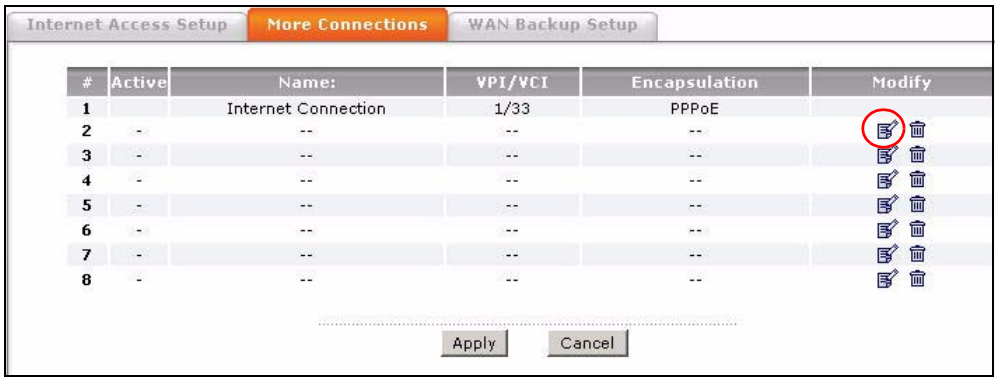
3 Click the **Advanced Setup** button to display the following options. Select **UBR** in the **ATM QoS Type** field.



4 Click **Apply**.

4.8.1.2 PVC 2 for VoIP Traffic

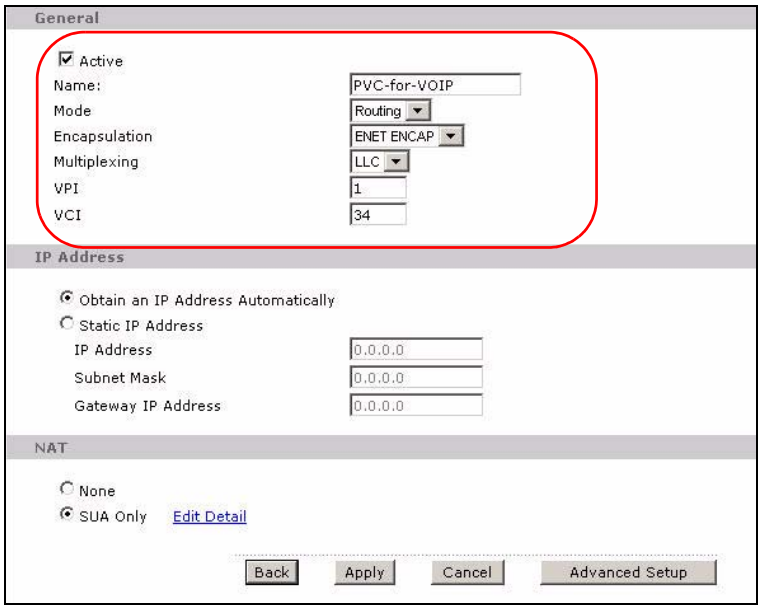
1 Click the **More Connections** tab and then click the **Edit** icon next to the entry two.


Internet Access Setup
More Connections
WAN Backup Setup
Active Name: VPI/VCI Encapsulation Modify
1 Internet Connection 1/33 PPPoE
2 - -- -- -- --
3 - -- -- -- --
4 - -- -- -- --
5 - -- -- -- --
6 - -- -- -- --
7 - -- -- -- --
8 - -- -- -- --
Apply
Cancel

2 Then configure the screen using the following example settings:

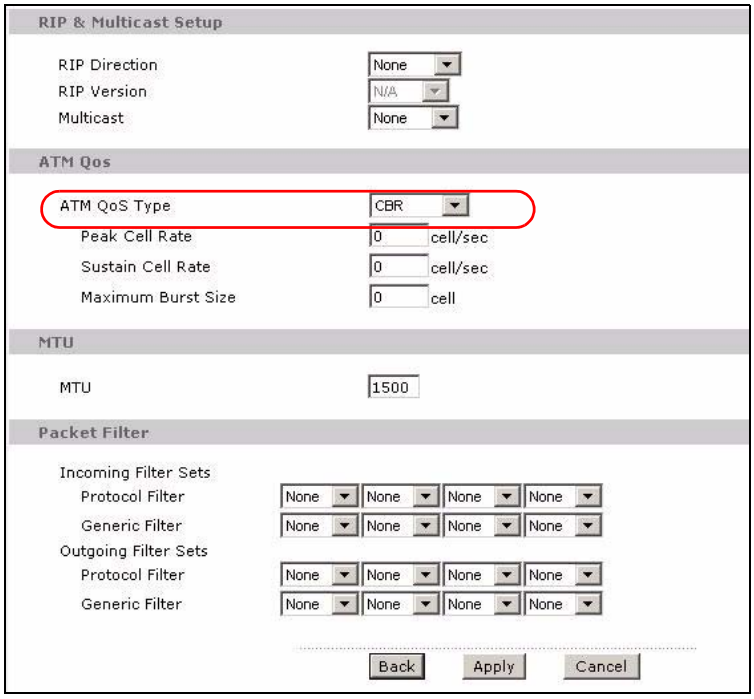
- Select **Active**.
- Name: **PVC-for-VoIP**
- Mode: **Routing**

- Encapsulation: **ENET ENCAP**
- PVC: **LLC**, **1/34**
- ATM QoS: **CBR**



3 Click **Apply**.

4 Click the **Advanced Setup** button and then select **CBR** in the **ATM QoS Type** field.



5 Click **Apply**.

4.8.2 Configuring QoS

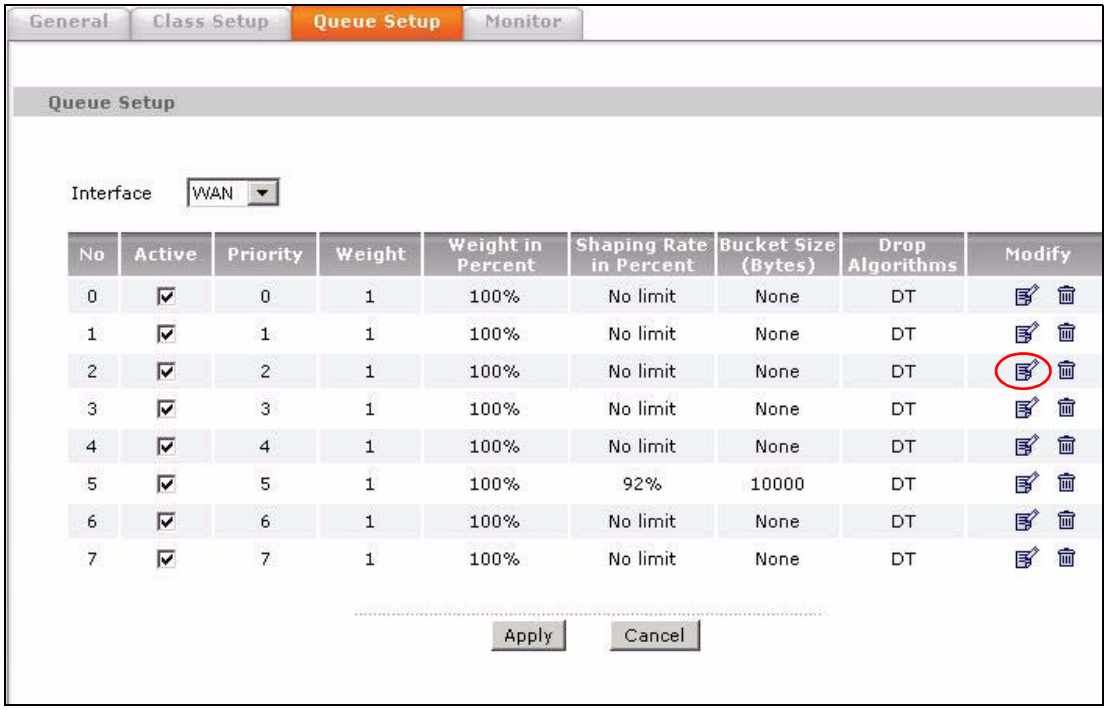
In this example, the maximum upstream transmission rate of the DSL port is 1 Mbps, with 70% being allocated to Internet access traffic and 92% (default shaping rate) for VoIP. (The shaping rate total can be more than 100%.) Internet access traffic is assigned queue 2 and VoIP traffic is assigned a higher priority of queue 5. The bucket size for Internet access traffic is set as 87,500 bytes and 100,000 bytes (maximum size) for VoIP traffic. Configure the screens as shown in the following sections with this information.

Table 10 QoS Queue Configuration

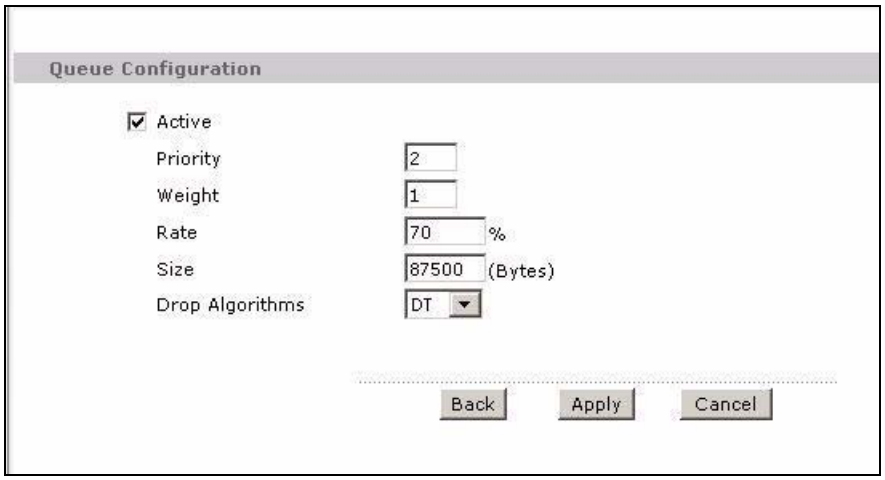
QUEUE NO.	SHAPING RATE IN PERCENT	BUCKET SIZE
2	70%	87,500 Bytes
5	92% (default)	100,000 Bytes

4.8.2.1 Queue Setup

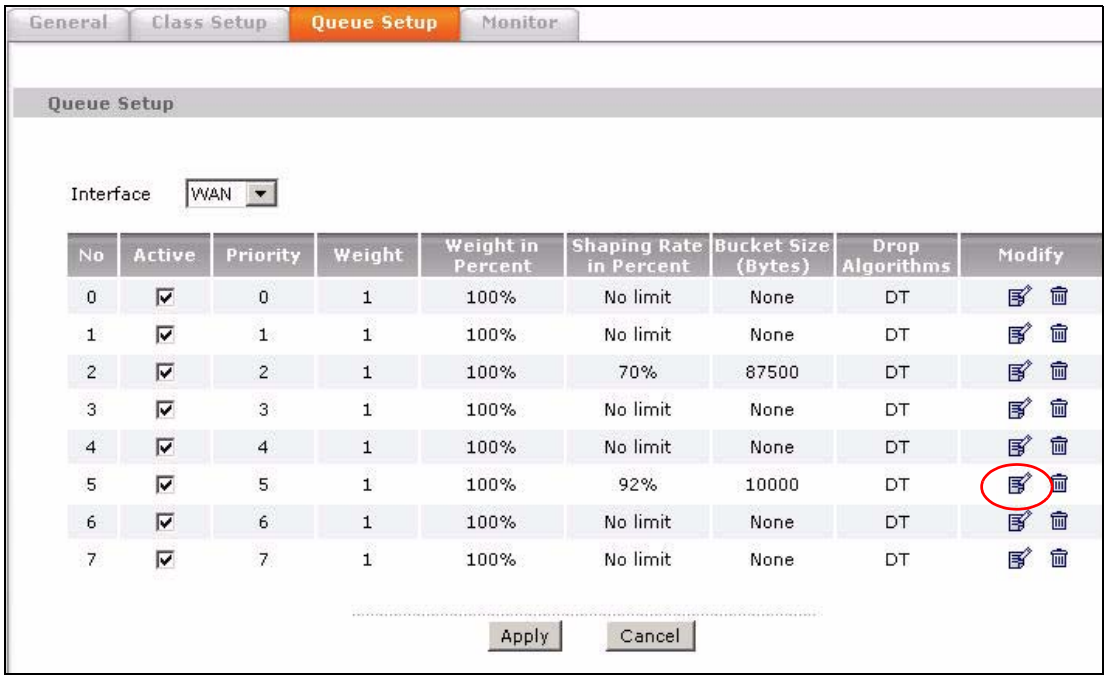
1 Click **Advanced** > **QoS** > **Queue Setup**. Click the **Edit** icon of queue 2 to open the Queue Configuration screen.



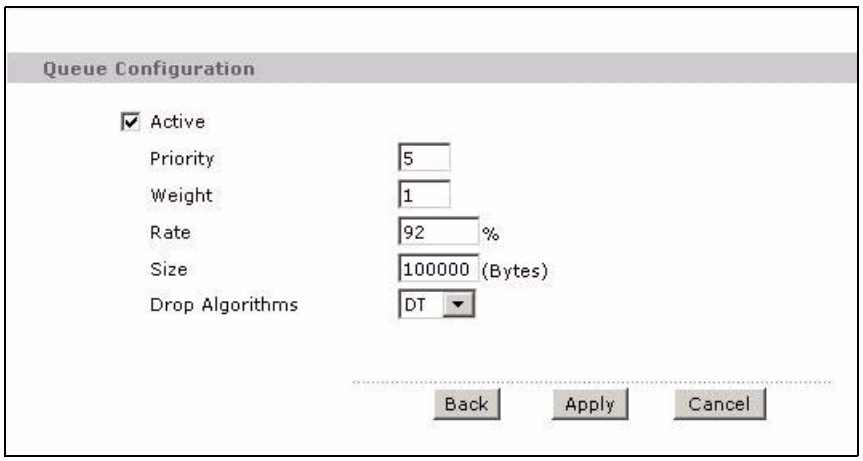
2 Enter 70 in the **Rate** field and 87500 in the **Size** field. Click **Apply**.



3 Click the **Edit** icon of queue 5 to open the **Queue Configuration** screen.



4 The **Rate** field is 92% as in default. Enter 100,000 (maximum size) in the **Size** field. Click **Apply**.

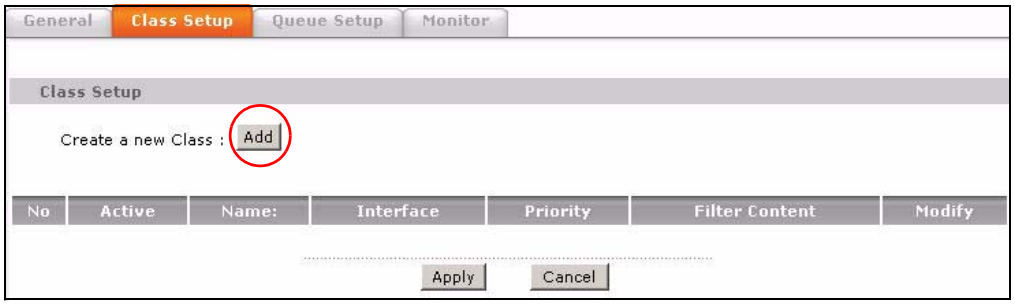


4.8.2.2 Class Setup

Now, configure these screens to identify the traffic you want to map to a PVC. In this tutorial, the ZyXEL Device maps traffic from LAN ports 1~3 to the Internet Access PVC with WAN Index 1 and traffic from LAN port 4 to the VoIP PVC with WAN index 2.

You could further refine traffic identification from a port by specifying VLAN tags, but this tutorial does not do that. See Chapter 15 on page 243 for how to configure VLAN groups.

1 Click **Advanced** > **QoS** > **Class Setup** and then click **Add** to create a QoS classifier rule for general data.



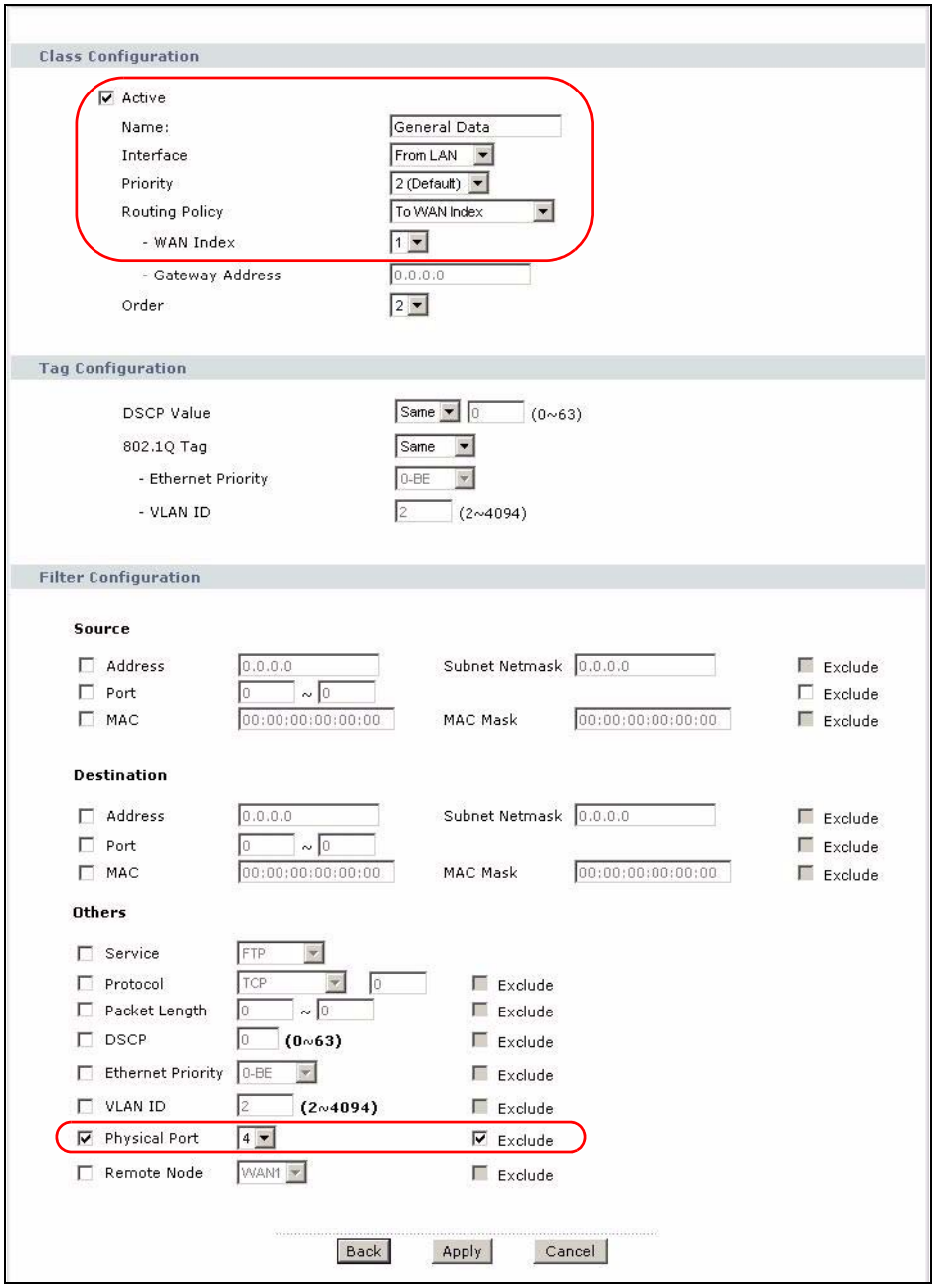
2 Configure this rule using the following example settings.

- Class Configuration:
  - Select **Active**.
  - Enter a descriptive name for this rule. For example, **General Data**.
  - Interface: **From LAN**
  - Priority: **2 (Default)**

- Routing Policy: **To WAN Index**
- WAN Index: **1**

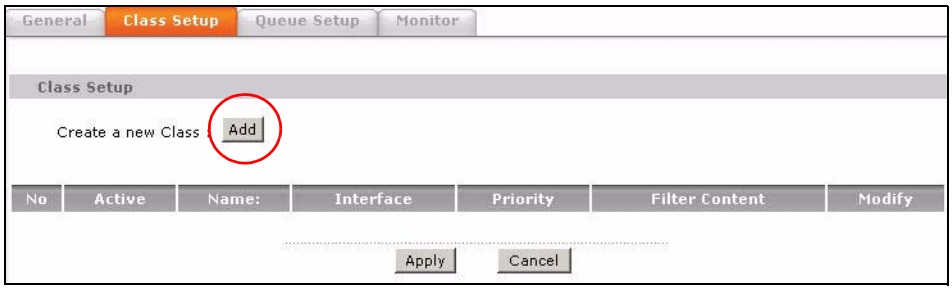
• Filter Configuration:

- Physical Port: 1~3 (exclude port 4)



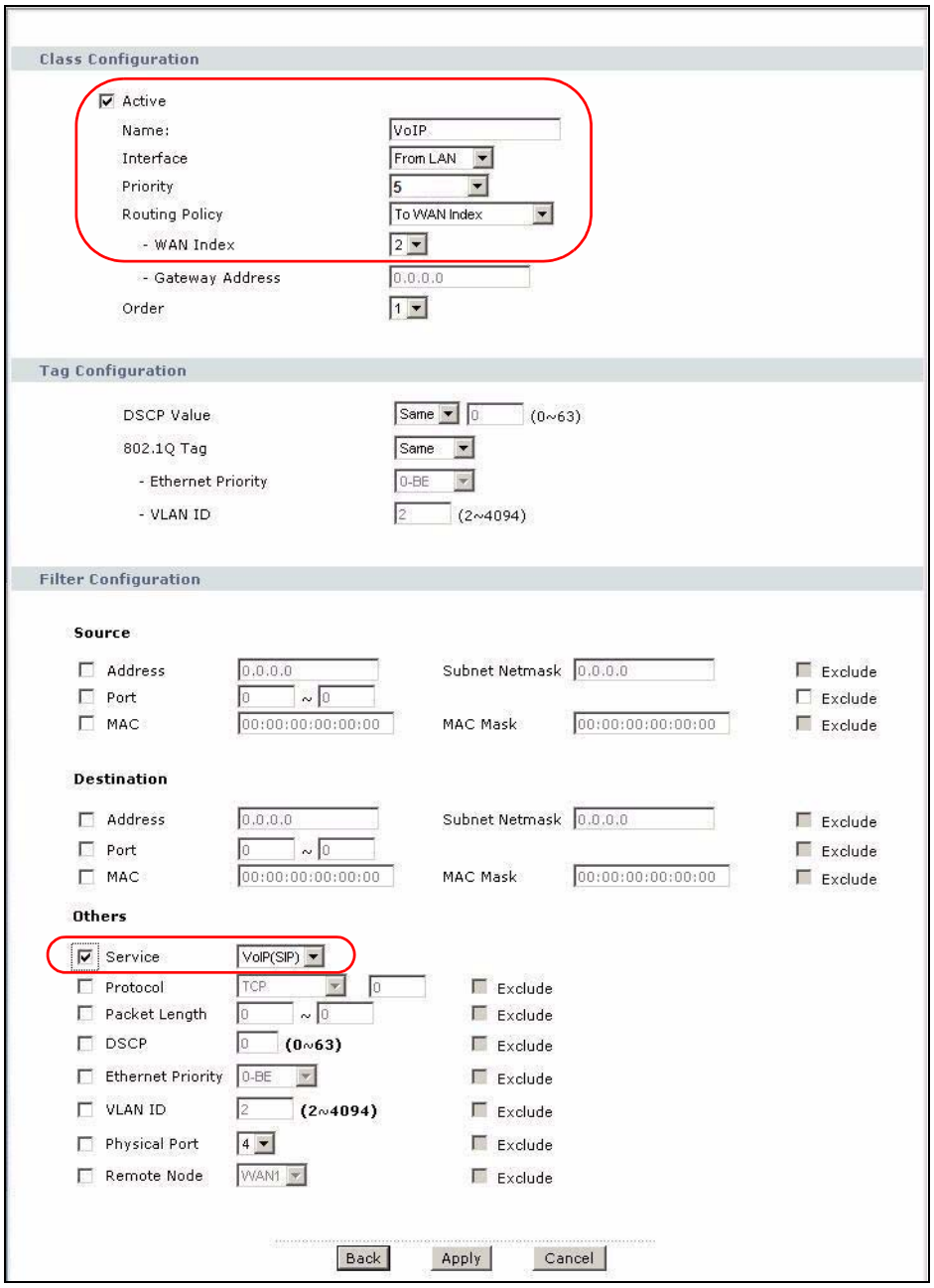
3 Click **Apply**.

4 Click **Add** to create another QoS classifier rule .



5 Create a class setup rule using the following example settings.

- Class Configuration:
  - Select **Active**.
  - Enter **VoIP** as the descriptive name for this rule.
  - Interface: **From LAN**
  - Priority: **5**
  - Routing Policy: **To WAN Index**
  - WAN Index: **2**
- Filter Configuration:
  - Service: **VoIP(SIP)**
  - Physical Port: **All**

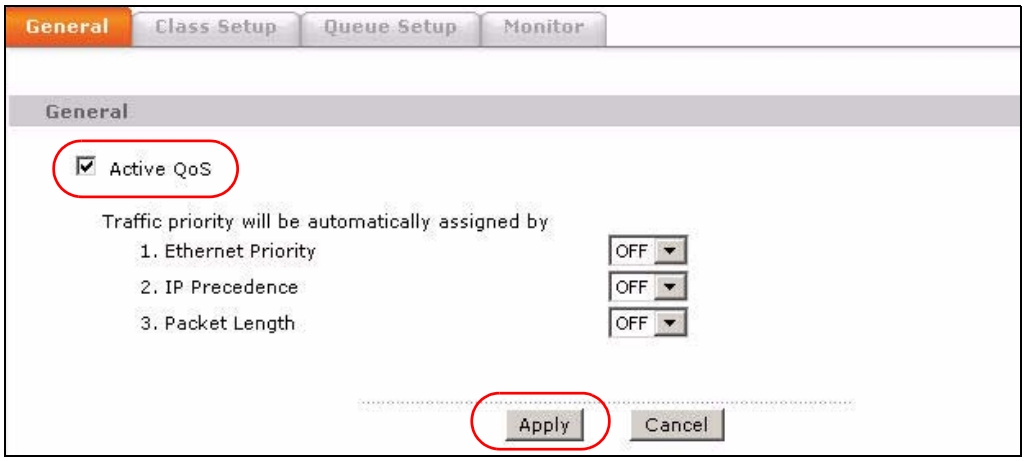


6 Click **Apply**.

4.8.2.3 Activate QoS on the ZyXEL Device

1 Click **Advanced** > **QoS** > **General**.

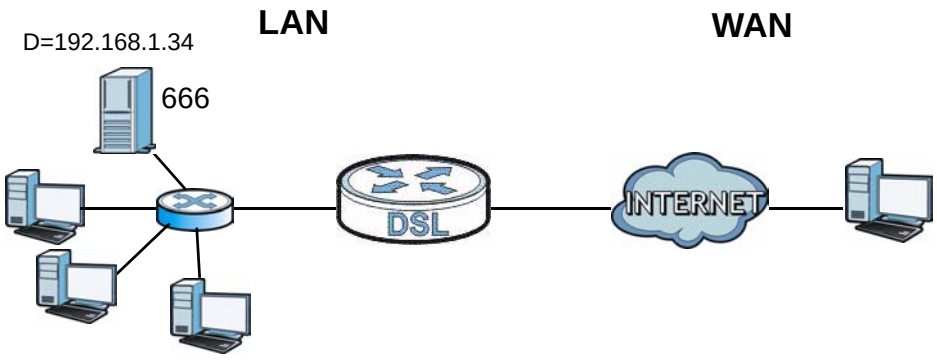
2 Select **Active QoS** and click **Apply**.



Now you can connect a VoIP phone to the ZyXEL Device's LAN port 4 and computers to port 1~3. The ZyXEL Device classifies and prioritizes voice traffic to optimize voice quality.

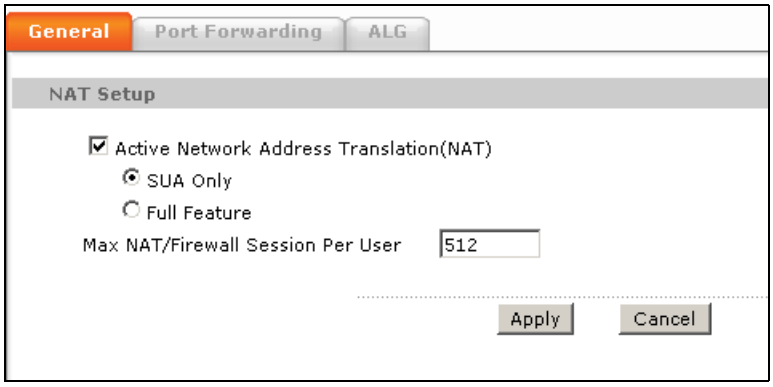
4.9 Setting Up NAT Port Forwarding

Thomas manages the Doom server on a computer behind the ZyXEL Device. In order for players on the Internet to communicate with the Doom server, Thomas needs to configure the port settings and IP address on the ZyXEL Device. Traffic should be forwarded to the port 666 of the Doom server computer which has an IP address of 192.168.1.34.

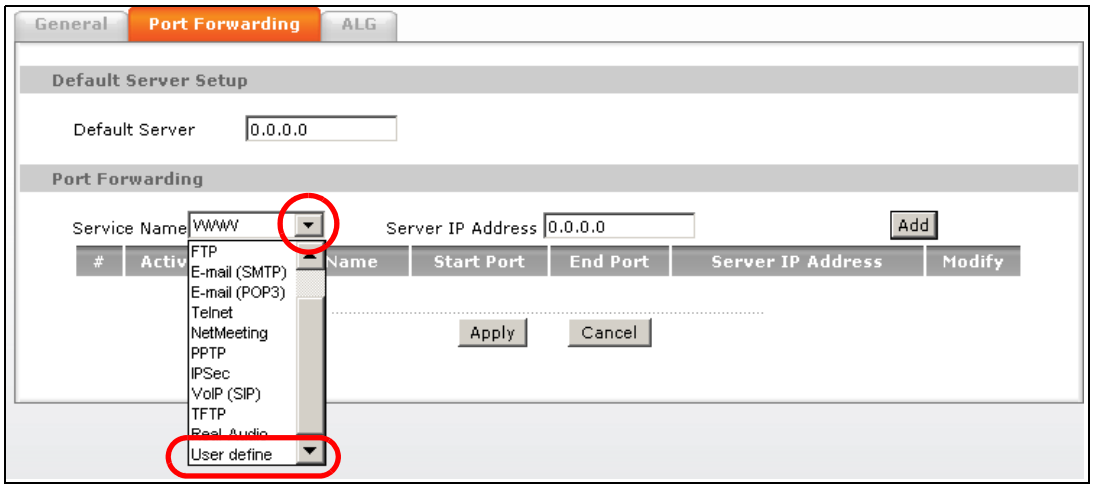


Thomas may set up the port settings by configuring the port settings for the Doom server computer (see Section on page 167 for more information).

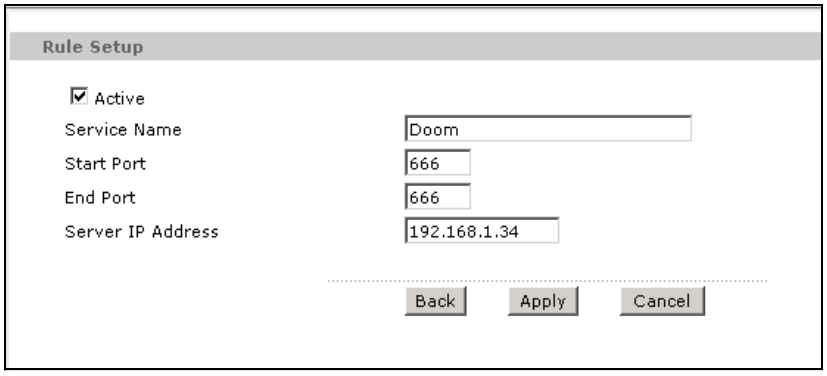
1 Click **Network** > **NAT** to open the **General** screen. Select **Active Network Address Translation** and **SUA Only**. Click **Apply**.



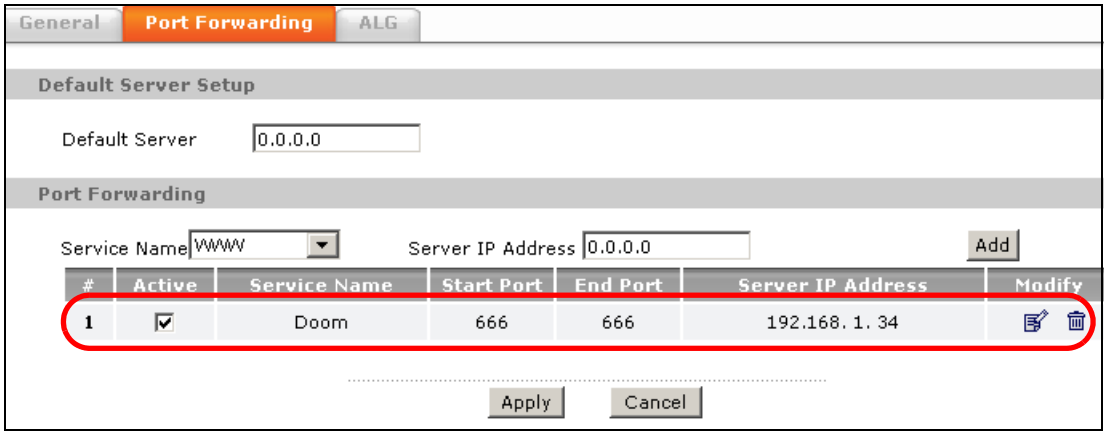
2 Click **Network** > **NAT** > **Port Forwarding** to open the following screen. Select **User define** from the **Service Name** field.



3 Configure the screen as follows to forward port 666 traffic to the computer with IP address 192.168.1.34. Click **Apply**.



4 The port forwarding settings you configured are listed in the **Port Forwarding** screen.



Players on the Internet then can have access to Thomas' Doom server.

PART II
Network

Internet (WAN) Setup (87)

Local Network (LAN) Setup (111)

Wireless LAN (129)

Network Address Translation (NAT) (163)

5

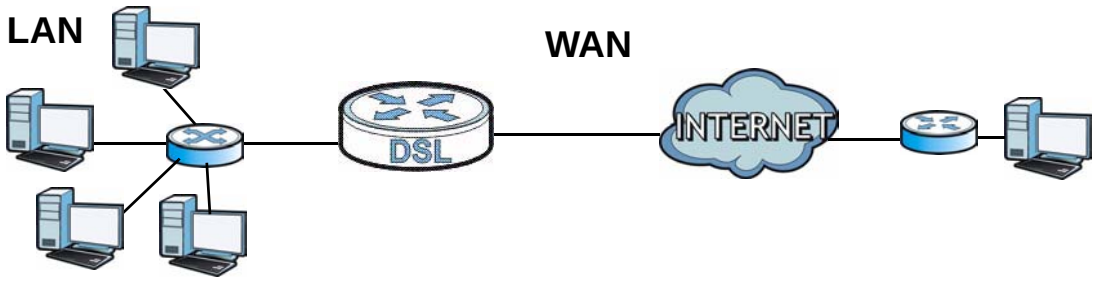
Internet (WAN) Setup

5.1 Overview

This chapter describes how to configure WAN settings from the **Internet (WAN)** screens. Use these screens to configure your ZyXEL Device for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks (such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 11 LAN and WAN



5.1.1 What You Can Do in the WAN Screens

- Use the **Internet Access Setup** screen (Section 5.2 on page 89) to configure the WAN settings on the ZyXEL Device for Internet access.
- Use the **More Connections** screen (Section 5.3 on page 95) to set up additional Internet access connections.
- Use the **WAN Backup Setup** screen to set up a backup gateway that helps forward traffic to its destination when the default WAN connection is down.

5.1.2 What You Need to Know About WAN

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the

same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPPoA, they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the ZyXEL Device, which makes it accessible from an outside network. It is used by the ZyXEL Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the ZyXEL Device tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just one.

IGMP

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 and 3 are improvements over version 1, but IGMP version 1 is still in wide use.

Finding Out More

See Section 5.5 on page 103 for technical background information on WAN.

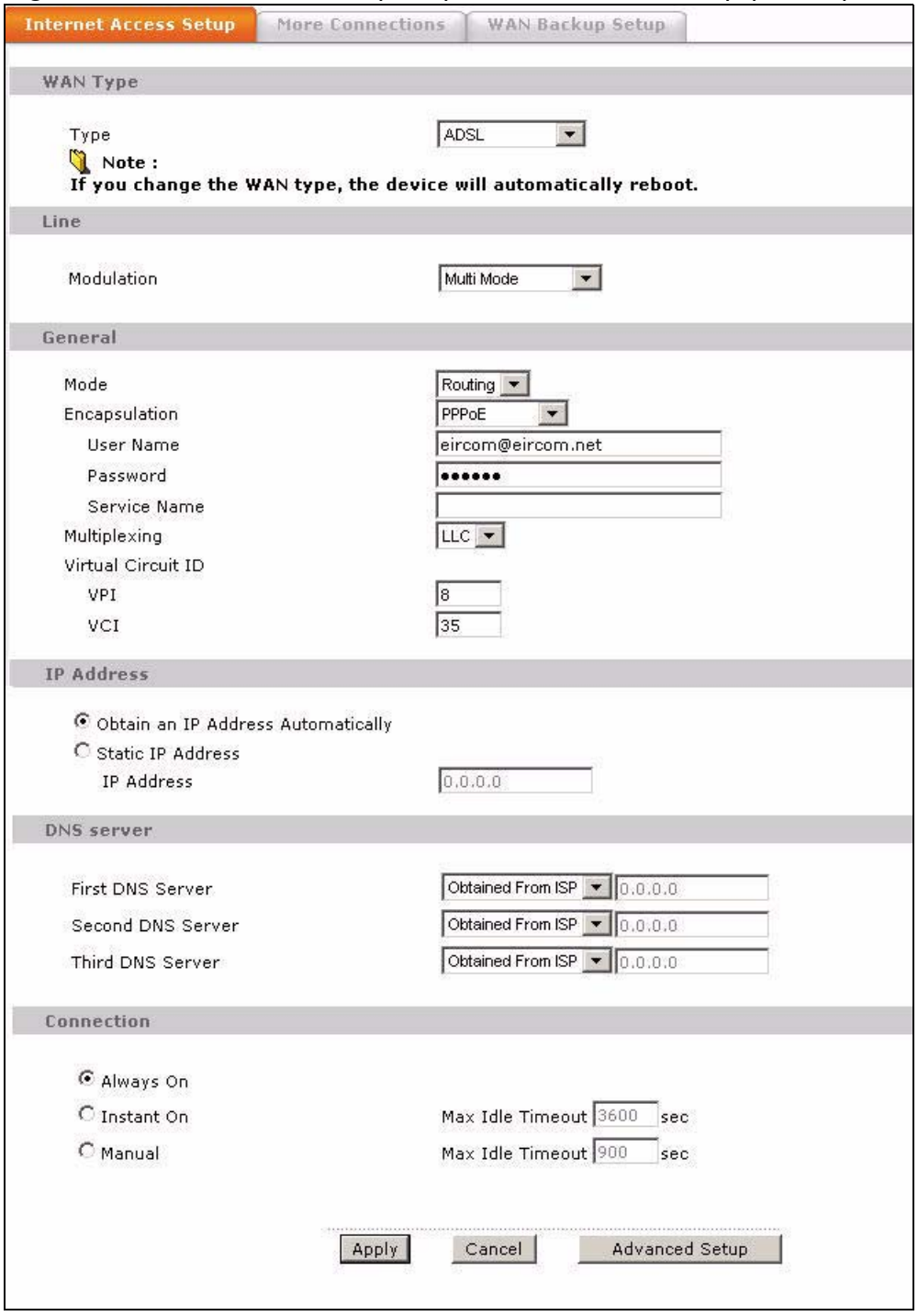
5.1.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

5.2 The Internet Access Setup Screen

Use this screen to change your ZyXEL Device's WAN settings. Click **Network > Internet (WAN) > Internet Access Setup**. The screen differs by the WAN type and encapsulation you select.

Figure 12 Network > Internet (WAN) >Internet Access Setup (PPPoE)



The following table describes the labels in this screen.

Table 11 Network > Internet (WAN) > Internet Access Setup

LABEL	DESCRIPTION
WAN Type	If you have a DSL modem or router in your network already, you can set the first Ethernet port as the WAN port and connect it to the DSL modem or router. This way, you can access the Internet via an Ethernet connection and still use the QoS, Firewall and VoIP functions on the ZyXEL Device.
Type	Select **ADSL** to use the DSL port on the ZyXEL Device. Select **Ethernet(ETH1)** to set the first Ethernet port as a WAN port. The DSL port will then be disabled automatically. This allows the ZyXEL Device to work as an Ethernet gateway, instead of a DSL router. To access the Internet, connect the first Ethernet port to a broadband modem or router. Note: Only LAN1 port can be used as Ethernet WAN port. Make sure your device is correctly connected. Note: The ZyXEL Device restarts after you change the setting in this field and click **Apply**.
Line	
Modulation	Select the modulation supported by your ISP. Use **Multi Mode** if you are not sure which mode to choose from. The ZyXEL Device dynamically diagnoses the mode supported by the ISP and selects the best compatible one for your connection. Other options are **ADSL G.dmt**, **ADSL2**, **ADSL2+**, **ADSL2 AnnexM**, **ADSL2+ AnnexM**, **READSL2 Mode**, **ANSI T1.413** and **ADSL G.lite**.
General	
Mode	Select **Routing** (default) from the drop-down list box if your ISP gives you one IP address only and you want multiple computers to share an Internet account. Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use Firewall, DHCP server and NAT on the ZyXEL Device.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.

Table 11 Network > Internet (WAN) > Internet Access Setup (continued)

LABEL	DESCRIPTION
Service Name	(PPPoE only) Type the name of your PPPoE service here.
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**. This field is not available if you set the WAN type to **Ethernet**.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information. These fields are not available if you set the WAN type to **Ethernet**.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address) and you select **Obtain an IP Address Automatically**. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. You must have another DNS server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Connection (PPPoA and PPPoE encapsulation only)	
Always On	Select **Always On** when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Instant On	Select **Instant On** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Manual	Select **Manual** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
Apply	Click this to save your changes.

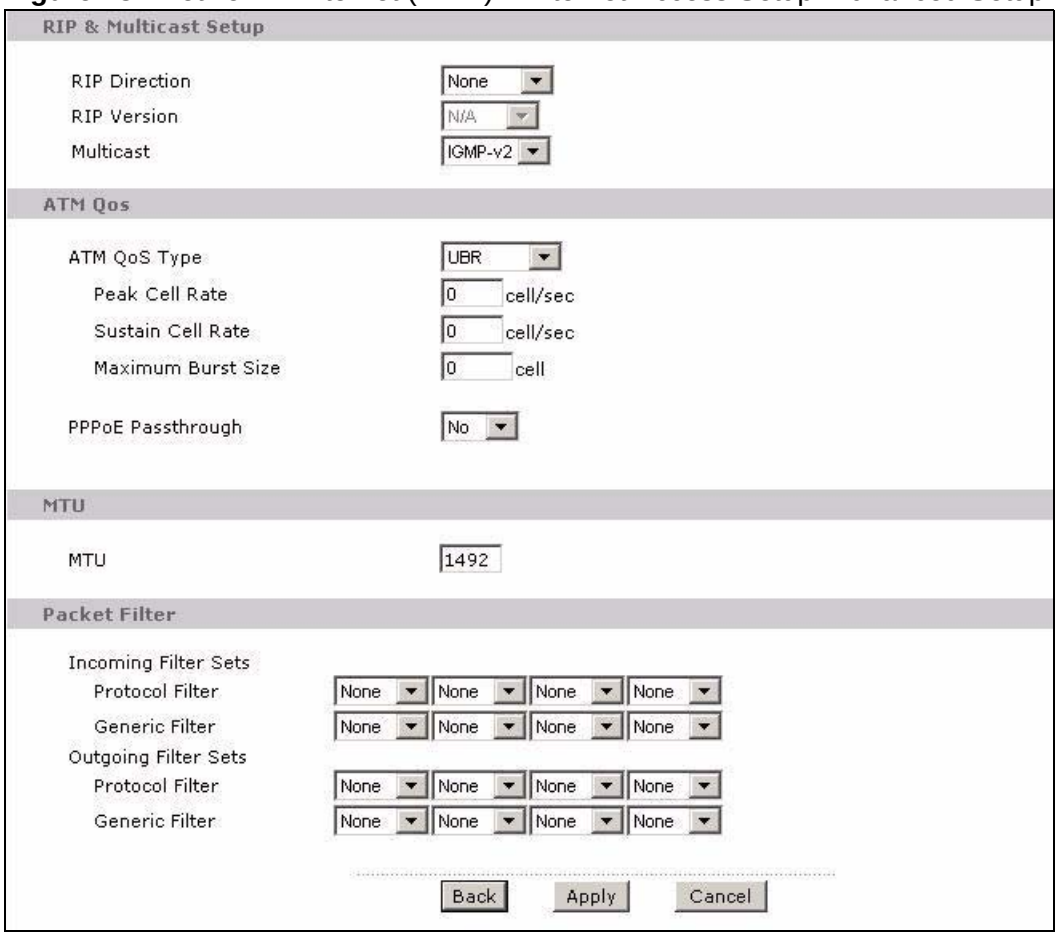
Table 11 Network > Internet (WAN) > Internet Access Setup (continued)

LABEL	DESCRIPTION
Cancel	Click this to restore your previously saved settings.
Advanced Setup	Click this to display the **Advanced WAN Setup** screen and edit more details of your WAN setup.

5.2.1 Advanced Internet Access Setup

Use this screen to edit your ZyXEL Device's advanced WAN settings. Click the **Advanced Setup** button in the **Internet Access Setup** screen. The screen appears as shown.

Figure 13 Network > Internet (WAN) > Internet Access Setup: Advanced Setup



The following table describes the labels in this screen.

Table 12 Network > Internet (WAN) > Internet Access Setup: Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	This section is not available when you configure the ZyXEL Device to be in bridge mode.
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	This field is not configurable if you select **None** in the **RIP Direction** field. Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer). Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports **IGMP-v1**, **IGMP-v2** and **IGMP-v3**. Select **None** to disable it.
ATM QoS	
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR-RT** (real-time Variable Bit Rate) type for applications with bursty connections that require closely controlled delay and delay variation. Select **VBR-nRT** (non real-time Variable Bit Rate) type for connections that do not require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.

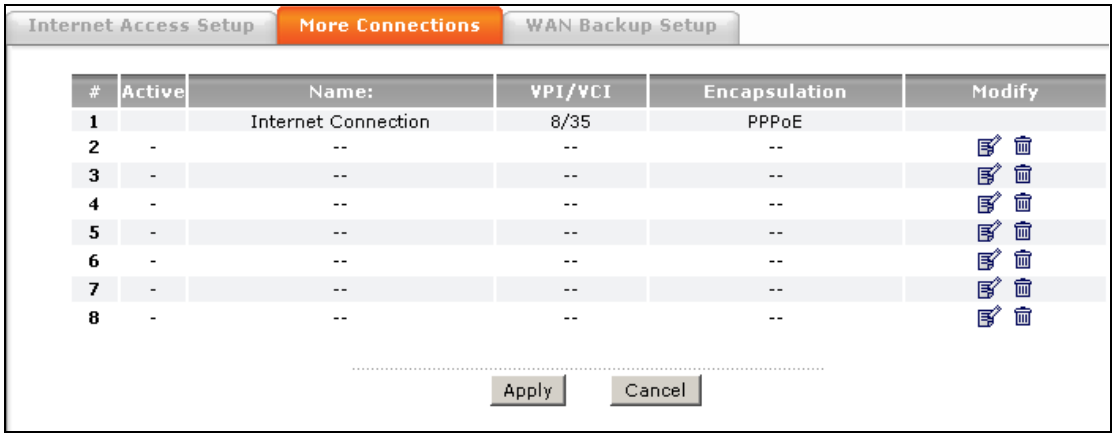
Table 12 Network > Internet (WAN) > Internet Access Setup: Advanced Setup

LABEL	DESCRIPTION
PPPoE Passthrough (PPPoE encapsulation only)	This field is available when you select **PPPoE** encapsulation. In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
MTU	
MTU	The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field. For ENET ENCAP, the MTU value is 1500. For PPPoE, the MTU value is 1492. For PPPoA and RFC 1483, the MTU is 65535.
Packet Filter	
Incoming Filter Sets	
Protocol Filter	Select the protocol filter(s) to control incoming traffic. You may choose up to 4 sets of filters. You can configure packet filters in the **Packet Filter** screen. See Chapter 11 on page 211 for more details.
Generic Filter	Select the generic filter(s) to control incoming traffic. You may choose up to 4 sets of filters. You can configure generic filters in the **Packet Filter** screen. See Chapter 11 on page 211 for more details.
Outgoing Filter Sets	
Protocol Filter	Select the protocol filter(s) to control outgoing traffic. You may choose up to 4 sets of filters. You can configure protocol filters in the **Packet Filter** screen. See Chapter 11 on page 211 for more details.
Generic Filter	Select the generic filter(s) to control outgoing traffic. You may choose up to 4 sets of filters. You can configure generic filters in the **Packet Filter** screen. See Chapter 11 on page 211 for more details.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

5.3 The More Connections Screen

The ZyXEL Device allows you to configure more than one Internet access connection. To configure additional Internet access connections click **Network > Internet (WAN) > More Connections**. The screen differs by the encapsulation you select. When you use the **Internet (WAN) > Internet Access Setup** screen to set up Internet access, you are configuring the first WAN connection.

Figure 14 Network > Internet (WAN) > More Connections


Internet Access Setup
More Connections
WAN Backup Setup
Active Name: VPI/VCI Encapsulation Modify
1 Internet Connection 8/35 PPPoE
2 - -- -- -- --
3 - -- -- -- --
4 - -- -- -- --
5 - -- -- -- --
6 - -- -- -- --
7 - -- -- -- --
8 - -- -- -- --
Apply
Cancel

The following table describes the labels in this screen.

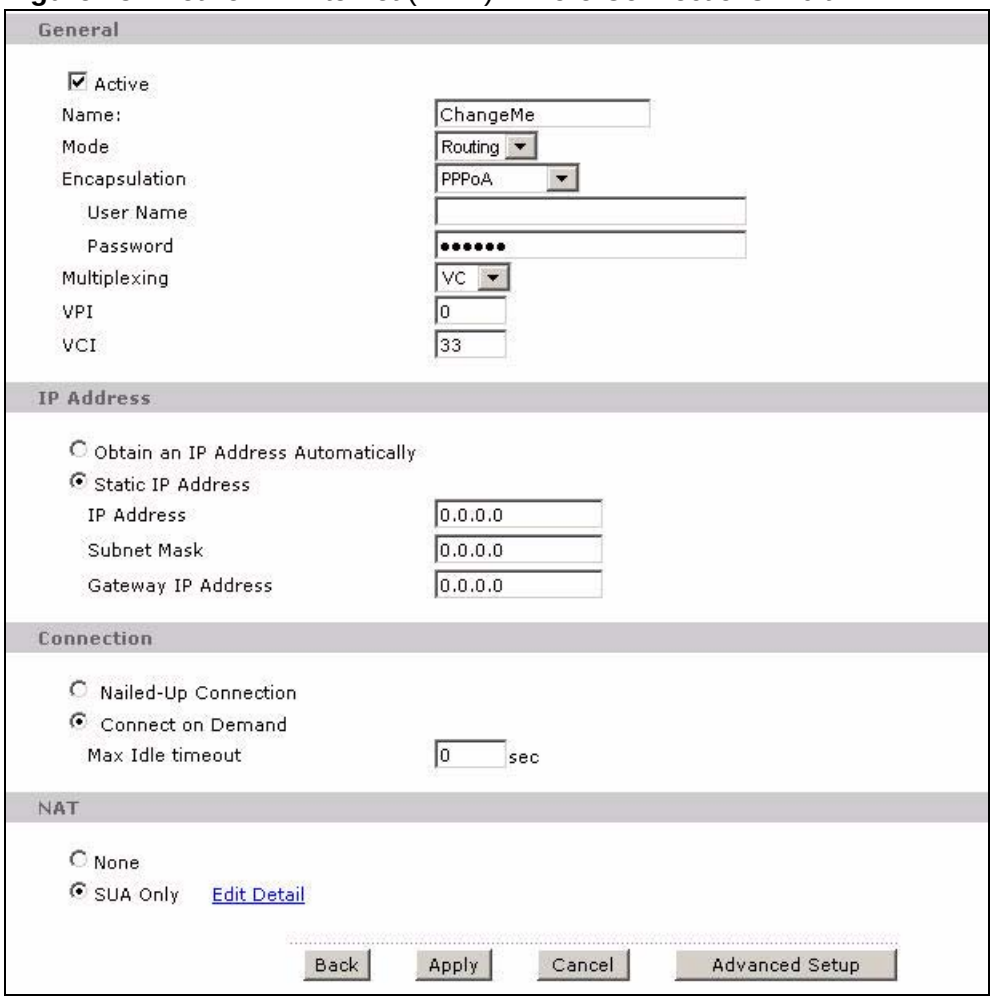
Table 13 Network > Internet (WAN) > More Connections

LABEL	DESCRIPTION
#	This is an index number indicating the number of the corresponding connection.
Active	This field indicates whether the connection is active or not. Clear the check box to disable the connection. Select the check box to enable it.
Name	This is the name you gave to the Internet connection.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers configured for this WAN connection.
Encapsulation	This field indicates the encapsulation method of the Internet connection.
Modify	The first (ISP) connection is read-only in this screen. Use the **Internet (WAN) > Internet Access Setup** screen to edit it. Click the Edit icon to edit the Internet connection settings. Click this icon on an empty configuration to add a new Internet access setup. Click the Remove icon to delete the Internet access setup from your connection list.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

5.3.1 More Connections Edit

Use this screen to configure a connection. Click the edit icon in the **More Connections** screen to display the following screen.

Figure 15 Network > Internet (WAN) > More Connections: Edit



The following table describes the labels in this screen.

Table 14 Network > Internet (WAN) > More Connections: Edit

LABEL	DESCRIPTION
General	
Active	Select the check box to activate or clear the check box to deactivate this connection.
Name	Enter a unique, descriptive name of up to 13 ASCII characters for this connection.

Table 14 Network > Internet (WAN) > More Connections: Edit (continued)

LABEL	DESCRIPTION
Mode	Select **Routing** from the drop-down list box if your ISP allows multiple computers to share an Internet account. If you select **Bridge**, the ZyXEL Device will forward any packet that it does not route to this remote node; otherwise, the packets are discarded.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**. By prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. If you select VC, specify separate VPI and VCI numbers for each protocol. For LLC-based multiplexing or PPP encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header. In this case, only one set of VPI and VCI numbers need be specified for all protocols.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. If you use the encapsulation type except **RFC 1483**, select **Obtain an IP Address Automatically** when you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below. If you use **RFC 1483**, enter the IP address given by your ISP in the **IP Address** field.
Subnet Mask	This option is available if you select **ENET ENCAP** in the **Encapsulation** field. Enter a subnet mask in dotted decimal notation.

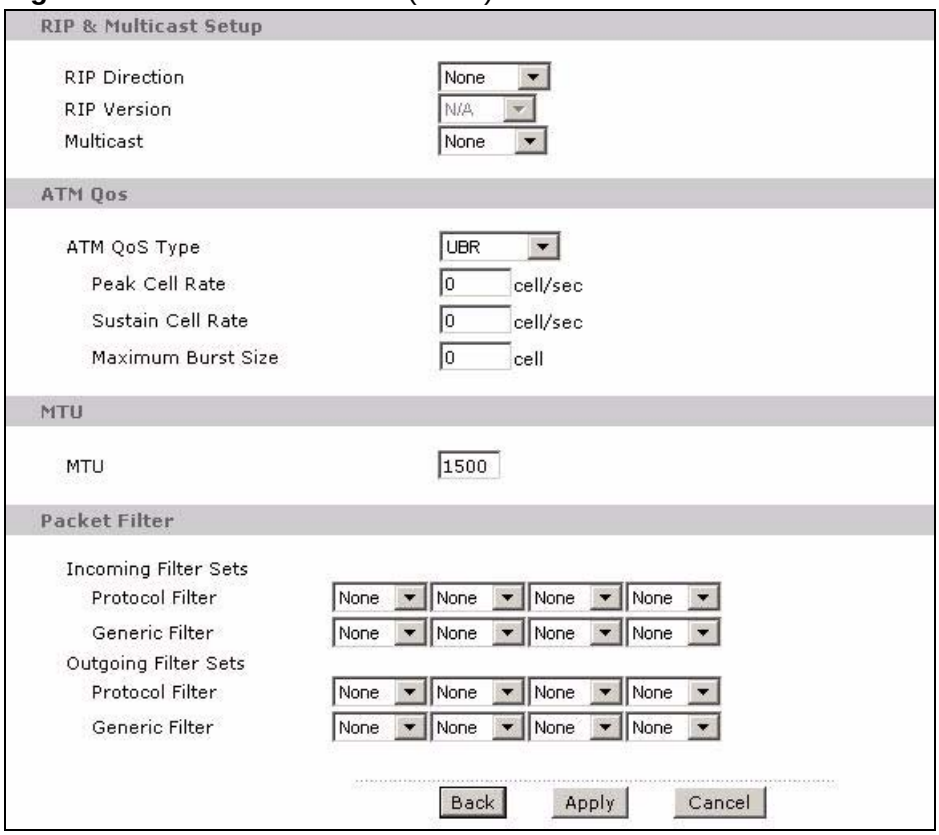
Table 14 Network > Internet (WAN) > More Connections: Edit (continued)

LABEL	DESCRIPTION
Gateway IP address	This option is available if you select **ENET ENCAP** in the **Encapsulation** field. Specify a gateway IP address (supplied by your ISP).
Connection	
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
NAT	**SUA only** is available only when you select **Routing** in the **Mode** field. Select **SUA Only** if you have one public IP address and want to use NAT. Click **Edit Detail** to go to the **Port Forwarding** screen to edit a server mapping set. Otherwise, select **None** to disable NAT.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced Setup	Click this to display the **More Connections Advanced Setup** screen and edit more details of your WAN setup.

5.3.2 Configuring More Connections Advanced Setup

Use this screen to edit your ZyXEL Device's advanced WAN settings. Click the **Advanced Setup** button in the **More Connections Edit** screen. The screen appears as shown.

Figure 16 Network > Internet (WAN) > More Connections: Edit: Advanced Setup



The following table describes the labels in this screen.

Table 15 Network > Internet (WAN) > More Connections: Edit: Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	This section is not available when you configure the ZyXEL Device to be in bridge mode.
RIP Direction	Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports **IGMP-v1**, **IGMP-v2** and **IGMP-v3**. Select **None** to disable it.
ATM QoS	

Table 15 Network > Internet (WAN) > More Connections: Edit: Advanced Setup

LABEL	DESCRIPTION
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR-nRT** (Variable Bit Rate-non Real Time) or **VBR-RT** (Variable Bit Rate-Real Time) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
MTU	
MTU	The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field. For ENET ENCAP, the MTU value is 1500. For PPPoE, the MTU value is 1492. For PPPoA and RFC, the MTU is 65535.
Packet Filter	
Incoming Filter Sets	
Protocol Filter	Select the protocol filter(s) to control incoming traffic. You may choose up to 4 sets of filters. You can configure packet filters in the **Packet Filter** screen. See Chapter 11 on page 211 for more details.
Generic Filter	Select the generic filter(s) to control incoming traffic. You may choose up to 4 sets of filters. You can configure generic filters in the **Packet Filter** screen. See Chapter 11 on page 211 for more details.
Outgoing Filter Sets	
Protocol Filter	Select the protocol filter(s) to control outgoing traffic. You may choose up to 4 sets of filters. You can configure protocol filters in the **Packet Filter** screen. See Chapter 11 on page 211 for more details.
Generic Filter	Select the generic filter(s) to control outgoing traffic. You may choose up to 4 sets of filters. You can configure generic filters in the **Packet Filter** screen. See Chapter 11 on page 211 for more details.
Back	Click this to return to the previous screen without saving.

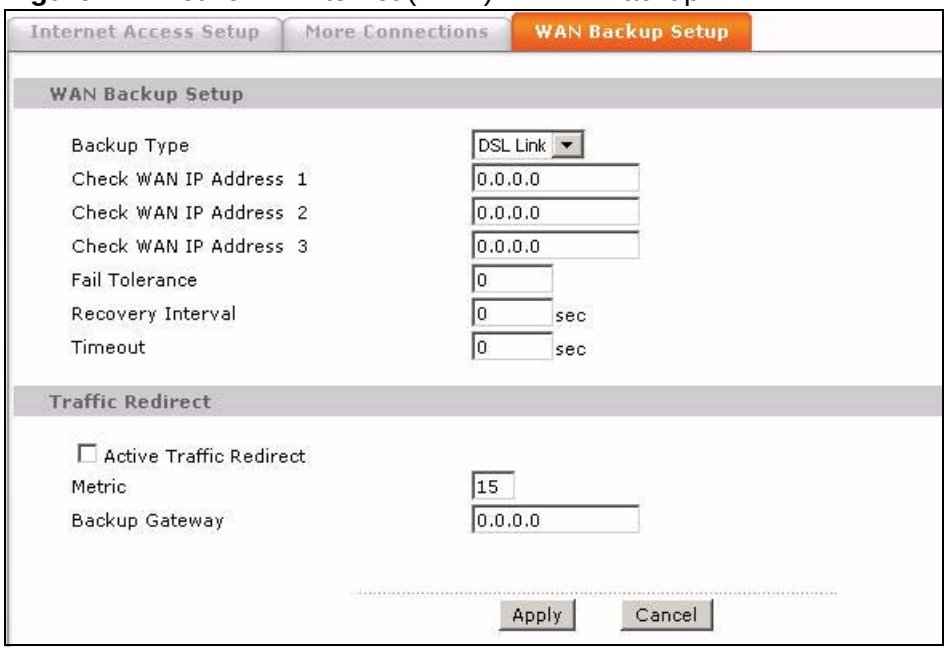
Table 15 Network > Internet (WAN) > More Connections: Edit: Advanced Setup

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

5.4 The WAN Backup Setup Screen

Use this screen to configure your ZyXEL Device's WAN backup. Click **Network > Internet (WAN) > WAN Backup Setup**. This screen is not available if you set the WAN type to **Ethernet** in the **Internet Access Setup** screen.

Figure 17 Network > Internet (WAN) > WAN Backup



The following table describes the labels in this screen.

Table 16 Network > Internet (WAN) > WAN Backup

LABEL	DESCRIPTION
Backup Type	Select the method that the ZyXEL Device uses to check the DSL connection. Select **DSL Link** to have the ZyXEL Device check if the connection to the DSLAM is up. Select **ICMP** to have the ZyXEL Device periodically ping the IP addresses configured in the **Check WAN IP Address** fields.
Check WAN IP Address1-3	Configure this field to test your ZyXEL Device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). If you activate either traffic redirect or dial backup, you must configure at least one IP address here. When using a WAN backup connection, the ZyXEL Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Fail Tolerance	Type the number of times (2 recommended) that your ZyXEL Device may ping the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval	When the ZyXEL Device is using a lower priority connection (usually a WAN backup connection), it periodically checks whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the ZyXEL Device to wait between checks. Allow more time if your destination IP address handles lots of traffic.
Timeout	Type the number of seconds (3 recommended) for your ZyXEL Device to wait for a ping response from one of the IP addresses in the **Check WAN IP Address** field before timing out the request. The WAN connection is considered "down" after the ZyXEL Device times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet.
Active Traffic Redirect	Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down. Note: If you activate traffic redirect, you must configure at least one Check WAN IP Address.

Table 16 Network > Internet (WAN) > WAN Backup

LABEL	DESCRIPTION
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

5.5 WAN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

5.5.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The ZyXEL Device supports the following methods.

5.5.1.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **Gateway IP Address** field in the wizard or WAN screen. You can get this information from your ISP.

5.5.1.2 PPP over Ethernet

The ZyXEL Device supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The PPPoE option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyXEL Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyXEL Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

5.5.1.3 PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The ZyXEL Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (Digital Subscriber Line (DSL) Access Multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

5.5.1.4 RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

5.5.2 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

5.5.3 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

5.5.4 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP gateway.

IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **Gateway IP Address** fields are not applicable (N/A). If you have a static IP, then you only need to fill in the **IP Address** field and not the **Gateway IP Address** field.

IP Assignment with RFC 1483 Encapsulation

In this case the IP address assignment must be static.

IP Assignment with ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the **IP Address** and **Gateway IP Address** fields as supplied by your ISP. However for a dynamic IP, the ZyXEL Device acts as a DHCP client on the WAN port and so the **IP Address** and **Gateway IP Address** fields are not applicable (N/A) as the DHCP server assigns them to the ZyXEL Device.

5.5.5 Nailed-Up Connection (PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyXEL Device does two things when you specify

a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyXEL Device will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

5.5.6 NAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

5.6 Metric

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the ZyXEL Device's routes to the Internet. If any two of the default routes have the same metric, the ZyXEL Device uses the following pre-defined priorities:

- Normal route: designated by the ISP (see Section 5.2 on page 89)
- Traffic-redirect route (see Section 5.9 on page 109)

For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the ZyXEL Device tries the traffic-redirect route next.

5.7 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

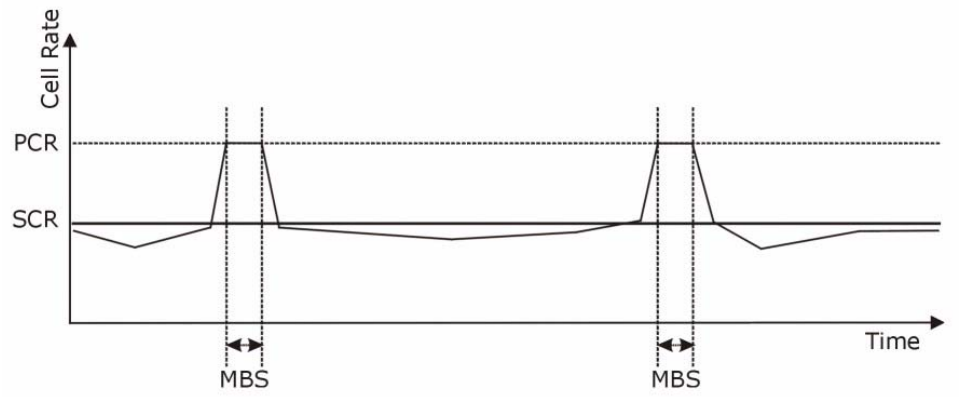
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 18 Example of Traffic Shaping



5.7.1 ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

5.8 Zero Configuration Internet Access

Once you turn on and connect the ZyXEL Device to a telephone jack, it automatically detects the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and makes the necessary configuration changes. In cases where additional account information (such as an Internet account user name and password) is required or the ZyXEL Device cannot connect to the ISP, you will be redirected to web screen(s) for information input or troubleshooting.

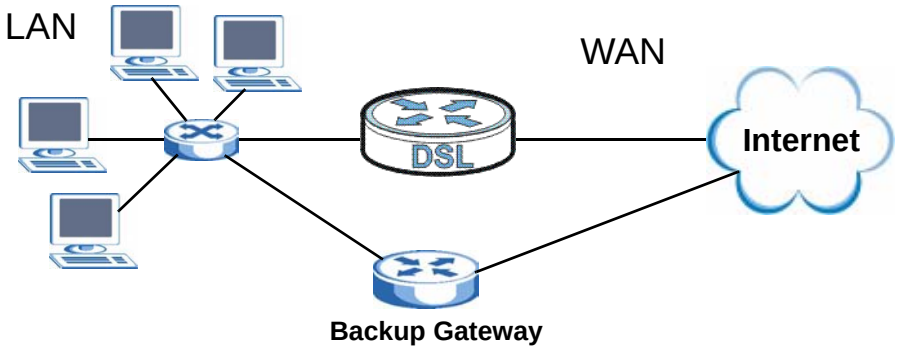
Zero configuration for Internet access is disabled when

- the ZyXEL Device is in bridge mode
- you set the ZyXEL Device to use a static (fixed) WAN IP address.

5.9 Traffic Redirect

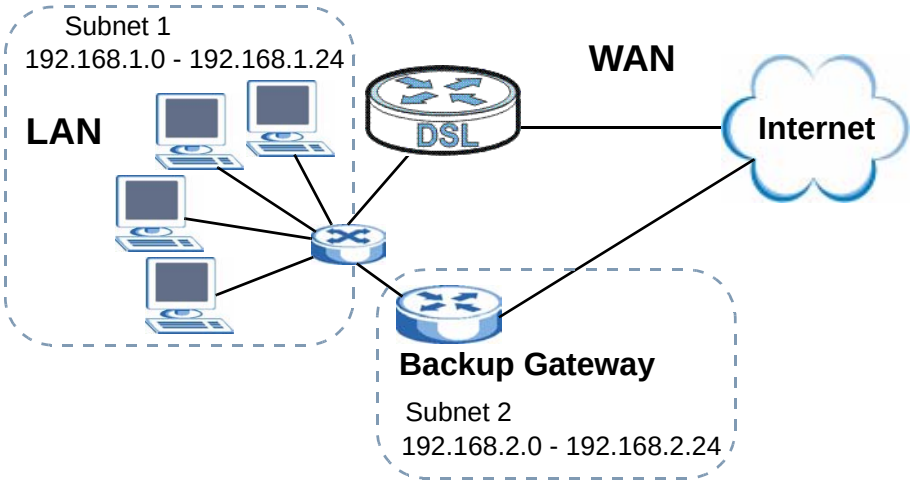
Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet. An example is shown in the figure below.

Figure 19 Traffic Redirect Example



The following network topology allows you to avoid triangle route security issues when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the ZyXEL Device itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure filters that allow packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

Figure 20 Traffic Redirect LAN Setup



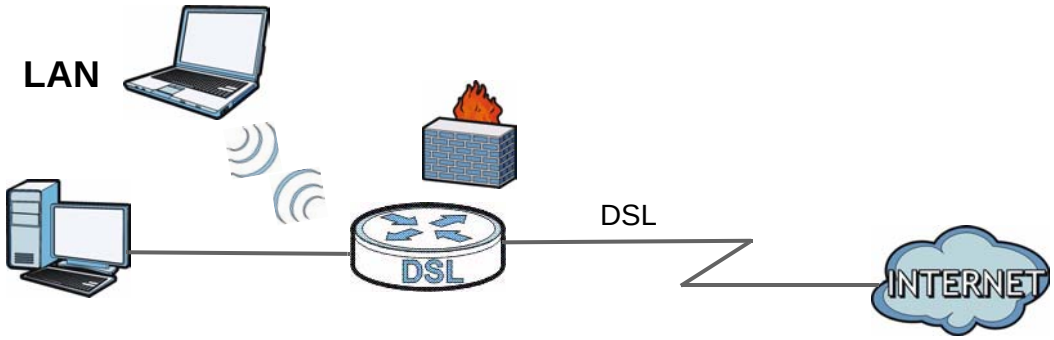
6

Local Network (LAN) Setup

6.1 Overview

A Local Area Network (LAN) is a shared communication system to which many networking devices are connected. It is usually located in one immediate area such as a building or floor of a building.

Use the LAN screens to help you configure a LAN DHCP server and manage IP addresses.



6.1.1 What You Can Do in the LAN Screens

- Use the **LAN IP** screen (Section 6.2 on page 113) to set the LAN IP address and subnet mask of your ZyXEL device. You can also edit your ZyXEL Device's RIP, multicast, any IP and Windows Networking settings from this screen.
- Use the **DHCP Setup** screen (Section 6.3 on page 116) to configure the ZyXEL Device's DHCP settings.
- Use the **Client List** screen (Section 6.4 on page 118) to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.
- Use the **IP Alias** screen (Section 6.5 on page 119) to change your ZyXEL Device's IP alias settings.

6.1.2 What You Need To Know About LAN

IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet Mask

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your ZyXEL Device an IP address, subnet mask, DNS and other routing information when it's turned on.

RIP

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.

Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 and 3 are improvements over version 1, but IGMP version 1 is still in wide use.

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a networking device before you can access it.

Finding Out More

See Section 6.6 on page 121 for technical background information on LANs.

6.1.3 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

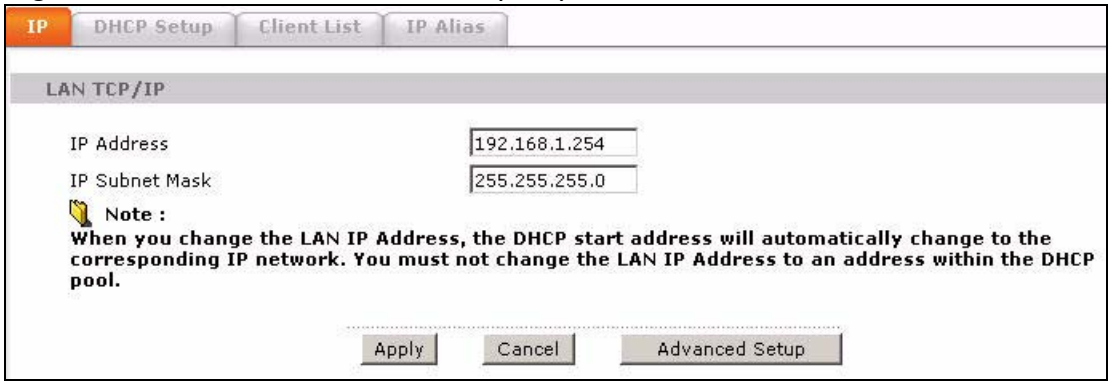
6.2 The LAN IP Screen

Use this screen to set the Local Area Network IP address and subnet mask of your ZyXEL Device. Click **Network > Local Network (LAN)** to open the **IP** screen.

Follow these steps to configure your LAN settings.

1. Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your ZyXEL Device.
2. Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.
3. Click **Apply** to save your settings.

Figure 21 Network > Local Network (LAN) > IP


IP
DHCP Setup
Client List
IP Alias
LAN TCP/IP
IP Address
192.168.1.254
IP Subnet Mask
255.255.255.0
Note :
When you change the LAN IP Address, the DHCP start address will automatically change to the corresponding IP network. You must not change the LAN IP Address to an address within the DHCP pool.
Apply
Cancel
Advanced Setup

The following table describes the fields in this screen.

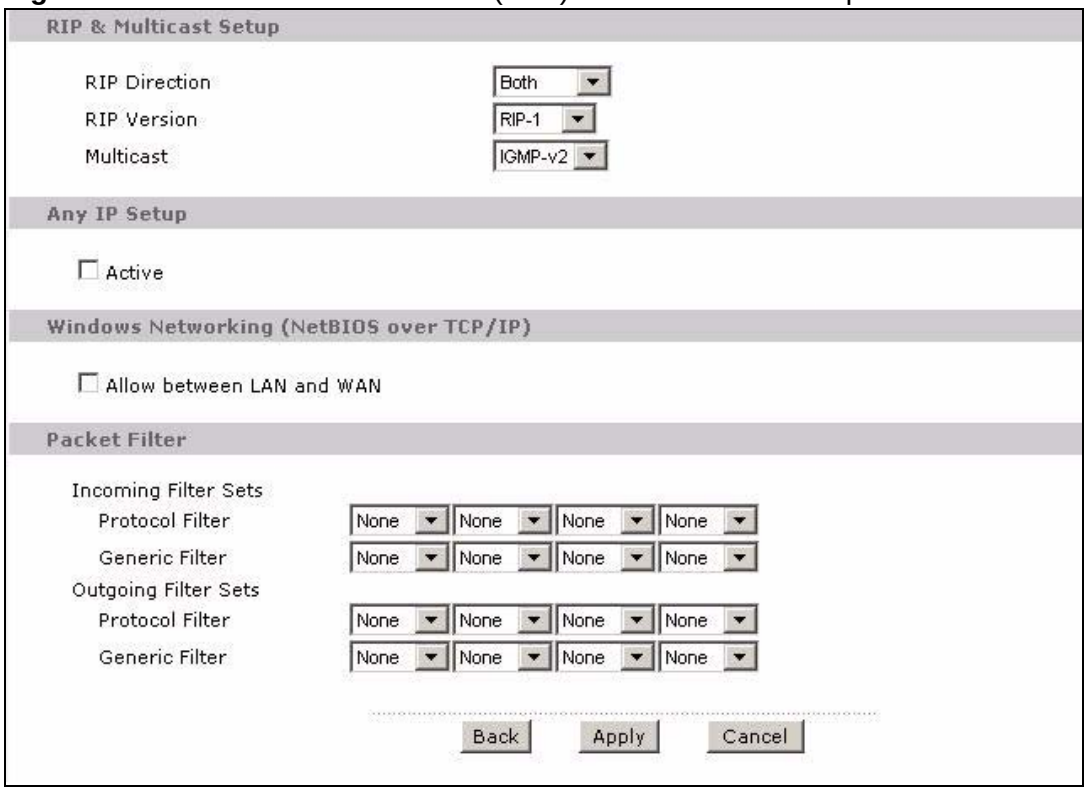
Table 17 Network > Local Network (LAN) > IP

LABEL	DESCRIPTION
IP Address	Enter the LAN IP address you want to assign to your ZyXEL Device in dotted decimal notation, for example, 192.168.1.254 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your ZyXEL Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced Setup	Click this to display the **Advanced LAN Setup** screen and edit more details of your LAN setup.

6.2.1 The Advanced LAN IP Setup Screen

Use this screen to edit your ZyXEL Device's RIP, multicast, Any IP and Windows Networking settings. Click the **Advanced Setup** button in the **LAN IP** screen. The screen appears as shown.

Figure 22 Network > Local Network (LAN) > IP: Advanced Setup



The following table describes the labels in this screen.

Table 18 Network > Local Network (LAN) > IP: Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports **IGMP-v1**, **IGMP-v2** and **IGMP-v3**. Select **None** to disable it.
Any IP Setup	Select the **Active** check box to enable the Any IP feature. This allows a computer to access the Internet via the ZyXEL Device without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet. When you disable the Any IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the ZyXEL Device's LAN IP address can connect to the ZyXEL Device or access the Internet through the ZyXEL Device. Note: You must enable NAT/SUA in the **NAT** screen to use the Any IP feature on the ZyXEL Device.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Packet Filter	
Incoming Filter Sets	
Protocol Filter	Select the protocol filter(s) to control incoming traffic. You may choose up to 4 sets of filters. You can configure packet filters in the **Packet Filter** screen. See Chapter 11 on page 211 for more details.
Generic Filter	Select the generic filter(s) to control incoming traffic. You may choose up to 4 sets of filters. You can configure generic filters in the **Packet Filter** screen. See Chapter 11 on page 211 for more details.
Outgoing Filter Sets	

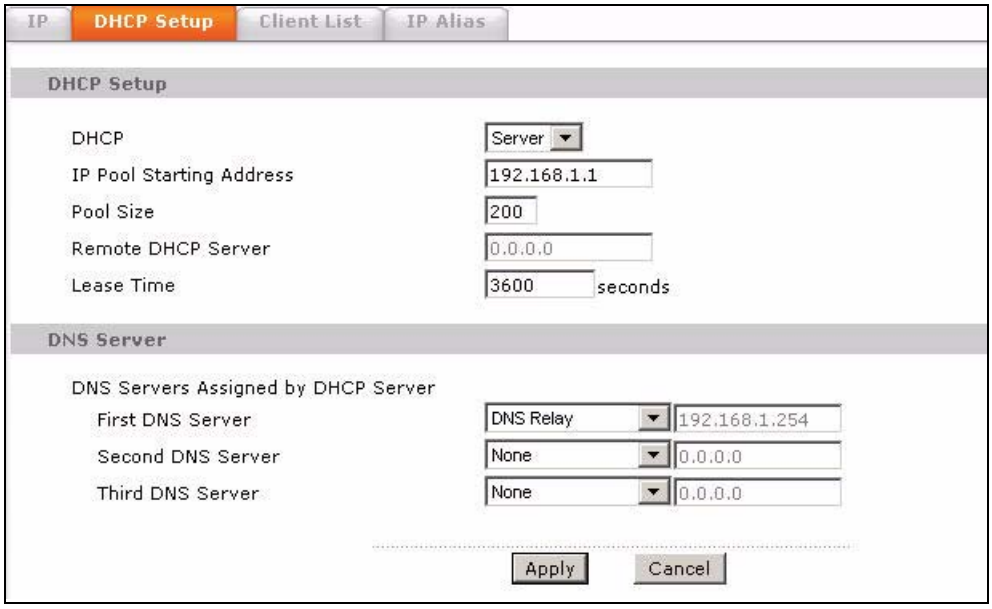
Table 18 Network > Local Network (LAN) > IP: Advanced Setup

LABEL	DESCRIPTION
Protocol Filter	Select the protocol filter(s) to control outgoing traffic. You may choose up to 4 sets of filters. You can configure protocol filters in the **Packet Filter** screen. See Chapter 11 on page 211 for more details.
Generic Filter	Select the generic filter(s) to control outgoing traffic. You may choose up to 4 sets of filters. You can configure generic filters in the **Packet Filter** screen. See Chapter 11 on page 211 for more details.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

6.3 The DHCP Setup Screen

Use this screen to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN. Click **Network > DHCP Setup** to open this screen.

Figure 23 Network > Local Network (LAN) > DHCP Setup



The following table describes the labels in this screen.

Table 19 Network > Local Network (LAN) > DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
DHCP	If set to **Server**, your ZyXEL Device can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the **Remote DHCP Server** field in this case. When DHCP is used, the following items need to be set:
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.
Lease Time	You can assign the DHCP lease time by entering the seconds manually. The lease time must be 10 seconds or more.
DNS Server	
DNS Servers Assigned by DHCP Server	The ZyXEL Device passes a DNS (Domain Name System) server IP address to the DHCP clients.
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the ZyXEL Device act as a DNS proxy only when the ISP uses IPCP DNS server extensions. The ZyXEL Device's LAN IP address displays in the field to the right (read-only). The ZyXEL Device tells the DHCP clients on the LAN that the ZyXEL Device itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select None if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.

Table 19 Network > Local Network (LAN) > DHCP Setup

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

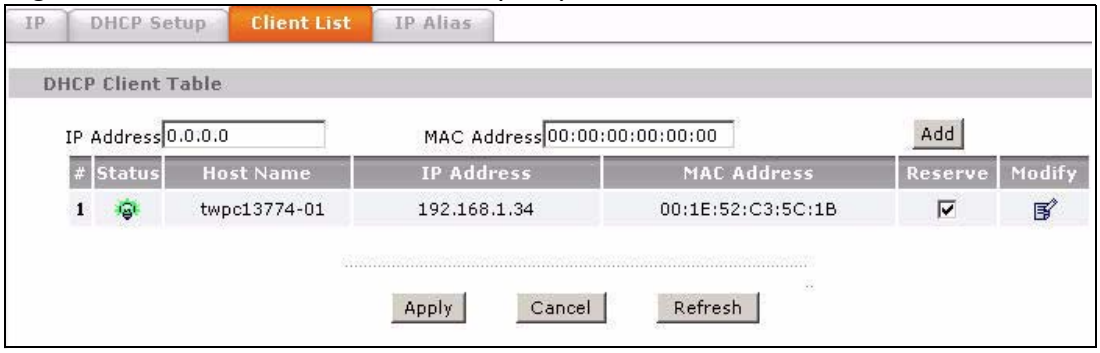
6.4 The Client List Screen

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Use this screen to change your ZyXEL Device's static DHCP settings. Click **Network > Local Network (LAN) > Client List** to open the following screen.

Figure 24 Network > Local Network (LAN) > Client List



The following table describes the labels in this screen.

Table 20 Network > Local Network (LAN) > Client List

LABEL	DESCRIPTION
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
MAC Address	Enter the MAC address of a computer on your LAN.
Add	Click this to add a static DHCP entry.
#	This is the index number of the static IP table entry (row).
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.

Table 20 Network > Local Network (LAN) > Client List

LABEL	DESCRIPTION
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 10 entries in this table.
Modify	Click the modify icon to have the IP address field editable and change it.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Refresh	Click this to reload the DHCP table.

6.5 The IP Alias Screen

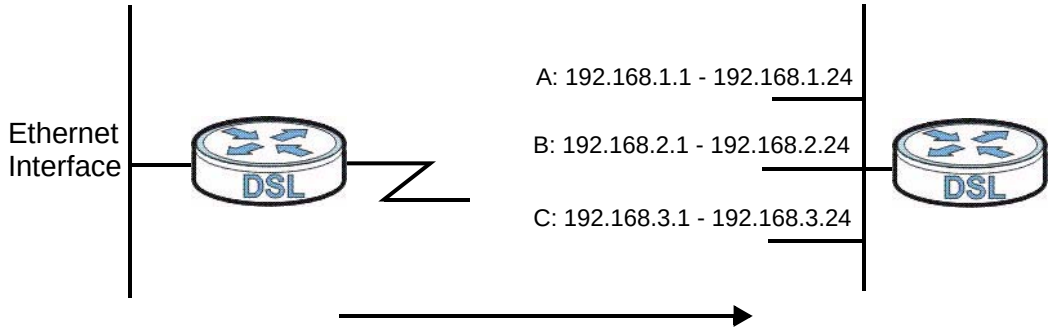
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

Note: Make sure that the subnets of the logical networks do not overlap.

The following figure shows a LAN divided into subnets A, B, and C.

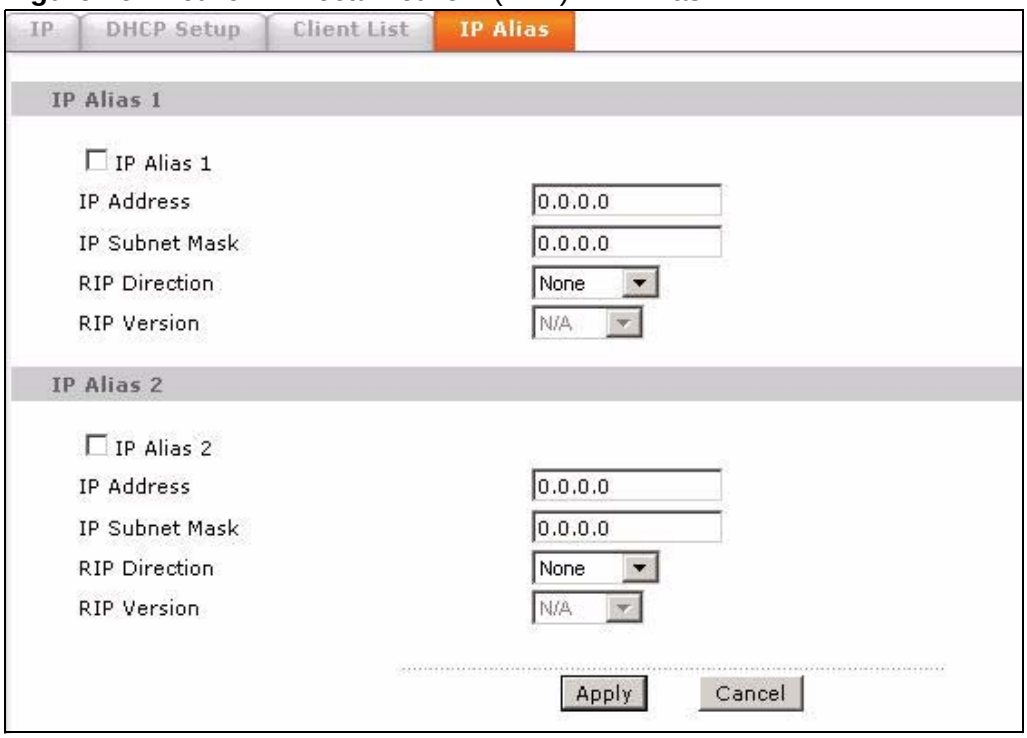
Figure 25 Physical Network & Partitioned Logical Networks



6.5.1 Configuring the LAN IP Alias Screen

Use this screen to change your ZyXEL Device's IP alias settings. Click **Network** > **Local Network (LAN)** > **IP Alias** to open the following screen.

Figure 26 Network > Local Network (LAN) > IP Alias



The following table describes the labels in this screen.

Table 21 Network > Local Network (LAN) > IP Alias

LABEL	DESCRIPTION
IP Alias 1, 2	Select the check box to configure another LAN network for the ZyXEL Device.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL Device will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

Table 21 Network > Local Network (LAN) > IP Alias

LABEL	DESCRIPTION
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

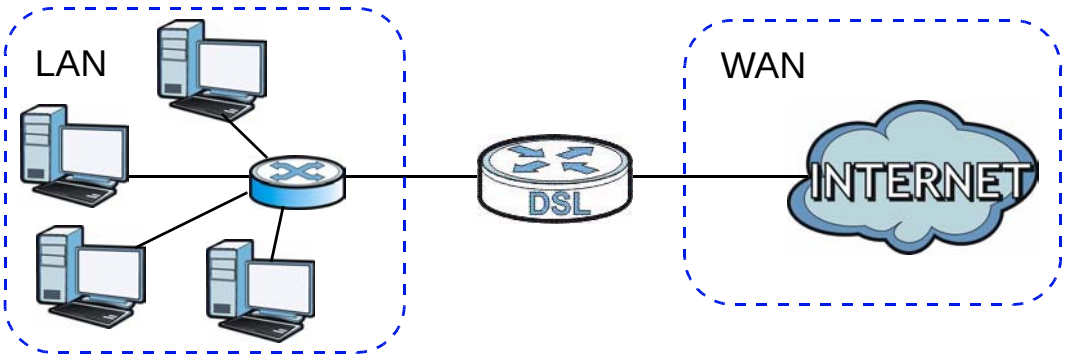
6.6 LAN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

6.6.1 LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the ZyXEL Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 27 LAN and WAN IP Addresses



6.6.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The ZyXEL Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

6.6.3 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ZyXEL Device supports the IPCP DNS server extensions through the DNS proxy feature.

  If the **DNS Server** fields in the **DHCP Setup** screen are set to **DNS Relay**, the ZyXEL Device tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the ZyXEL Device, the ZyXEL Device acts as a DNS proxy and forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

  Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

6.6.4 LAN TCP/IP

The ZyXEL Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyXEL Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255

- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, “Address Allocation for Private Internets” and RFC 1466, “Guidelines for Management of IP Address Space”.

6.6.5 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both -** the ZyXEL Device will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only -** the ZyXEL Device will not send any RIP packets but will accept all RIP packets received.
- **Out Only -** the ZyXEL Device will send out RIP packets but will not accept any RIP packets received.
- **None -** the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting.

6.6.6 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. IGMP version 3 supports source filtering, reporting or ignoring traffic from specific source address to a particular host on the network. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyXEL Device supports IGMP version 1 (**IGMP-v1**), IGMP version 2 (**IGMP-v2**) and IGMP version 3 (**IGMP-v3**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/ disabled on the ZyXEL Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

6.6.7 Any IP

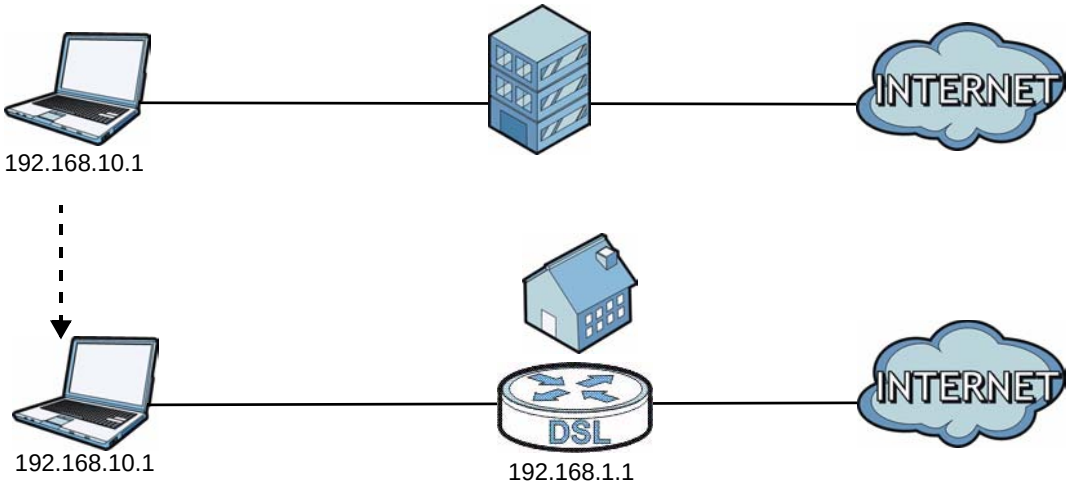
Traditionally, you must set the IP addresses and the subnet masks of a computer and the ZyXEL Device to be in the same subnet to allow the computer to access the Internet (through the ZyXEL Device). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the ZyXEL Device.

With the Any IP feature and NAT enabled, the ZyXEL Device allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the ZyXEL Device are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the ZyXEL Device and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a ZyXEL Device is installed, you can still use the computer to access the Internet

without changing the network settings, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.

Figure 28 Any IP Example



The Any IP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the ZyXEL Device's IP address.

Note: You must enable NAT/SUA to use the Any IP feature on the ZyXEL Device.

How Any IP Works

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the ZyXEL Device) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the ZyXEL Device.

1. When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the ZyXEL Device) by looking at the MAC address in its ARP table.
2. When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.
3. The ZyXEL Device receives the ARP request and replies to the computer with its own MAC address.

4 The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the ZyXEL Device.

5 When the ZyXEL Device receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

After all the routing information is updated, the computer can access the ZyXEL Device and the Internet as if it is in the same subnet as the ZyXEL Device.

7

Wireless LAN

7.1 Overview

This chapter describes how to perform tasks related to setting up and optimizing your wireless network, including the following.

- Turning the wireless connection on or off.
- Configuring a name, wireless channel and security for the network.
- Using WiFi Protected Setup (WPS) to configure your wireless network.
- Setting up multiple wireless networks.
- Using a MAC (Media Access Control) address filter to restrict access to the wireless network.
- Setting up a Wireless Distribution System (WDS).
- Performing other performance-related wireless tasks.

7.1.1 What You Can Do in the Wireless LAN Screens

This section describes the ZyXEL Device's **Network > Wireless LAN** screens. Use these screens to set up your ZyXEL Device's wireless connection.

- Use the **AP** screen (see Section 7.2 on page 131) to turn the wireless connection on or off, set up wireless security, configure the MAC filter, and make other basic configuration changes.
- Use the **More AP** screen (see Section 7.3 on page 140) to set up multiple wireless networks on your ZyXEL Device.
- Use the **WPS** screen (see Section 7.4 on page 143) to enable or disable WPS, generate a security PIN (Personal Identification Number) and see information about the ZyXEL Device's WPS status.
- Use the **WPS Station** (see Section 7.5 on page 144) screen to set up WPS by pressing a button or using a PIN.
- Use the **WDS** screen (see Section 7.6 on page 145) to set up a Wireless Distribution System, in which the ZyXEL Device acts as a bridge with other ZyXEL access points.
- Use the **Scheduling** screen (see Section 7.7 on page 147) to configure the dates/times to enable or disable the wireless LAN.

You don't necessarily need to use all these screens to set up your wireless connection. For example, you may just want to set up a network name, a wireless radio channel and security in the **AP** screen.

7.1.2 What You Need to Know About Wireless

Wireless Basics

"Wireless" is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there a number of wireless networking standards available with different methods of data encryption.

SSID

Each network must have a name, referred to as the SSID - "Service Set IDentifier". The "service set" is the network, so the "service set identifier" is the network's name. This helps you identify your wireless network when wireless networks' coverage areas overlap and you have a variety of networks to choose from.

MAC Address Filter

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address consists of twelve hexadecimal characters (0-9, and A to F), and it is usually written in the following format: "0A:A0:00:BB:CC:DD".

The MAC address filter controls access to the wireless network. You can use the MAC address of each wireless client to allow or deny access to the wireless network.

Finding Out More

See Section 7.8 on page 147 for advanced technical information on wireless networks.

7.1.3 Before You Start

Before you start using these screens, ask yourself the following questions. See Section 7.1.2 on page 130 if some of the terms used here are not familiar to you.

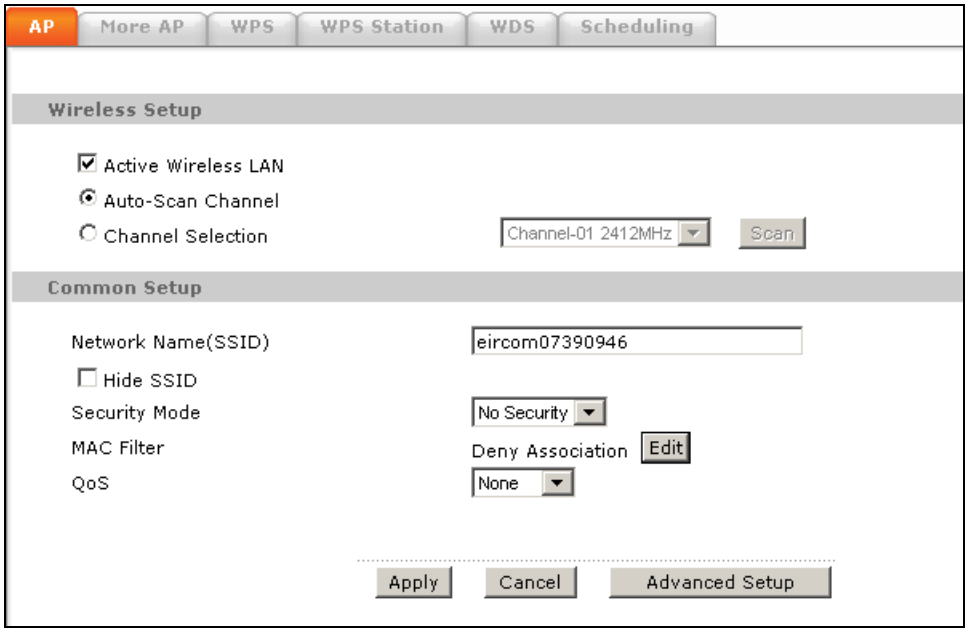
- What wireless standards do the other wireless devices in your network support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices in your network support (WPA-PSK, for example)? What is the strongest security option supported by all the devices in your network?
- Do the other wireless devices in your network support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

  Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.
- What advanced options do you want to configure, if any? If you want to configure advanced options such as Quality of Service, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them as they are.

7.2 The AP Screen

Use this screen to configure the wireless settings of your ZyXEL Device. Click **Network > Wireless LAN** to open the **AP** screen.

Figure 29 Network > Wireless LAN > AP



The following table describes the labels in this screen.

Table 22 Network > Wireless LAN > AP

LABEL	DESCRIPTION
Wireless Setup	
Active Wireless LAN	Click the check box to activate wireless LAN.
Auto-Scan Channel	Select this option to have the ZyXEL Device automatically scan for and select a channel which is not used by another device.
Channel Selection	Set the operating frequency/channel depending on your particular region. Click the **Scan** button to list available channels and then select a channel from the drop-down list box.
Common Setup	
Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. The default SSID is dependent on the ZyXEL Device's MAC address and is in the format eircomxxxxxxxx for example, eircom07390946. This will be printed on a label on the bottom of the device. If you want to change it, enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Security Mode	See the following sections for more details about this field.
MAC Filter	This shows whether the wireless devices with the MAC addresses listed are allowed or denied to access the ZyXEL Device using this SSID.
Edit	Click this to go to the **MAC Filter** screen to configure MAC filter settings. See Section 7.2.6 on page 139 for more details.

Table 22 Network > Wireless LAN > AP

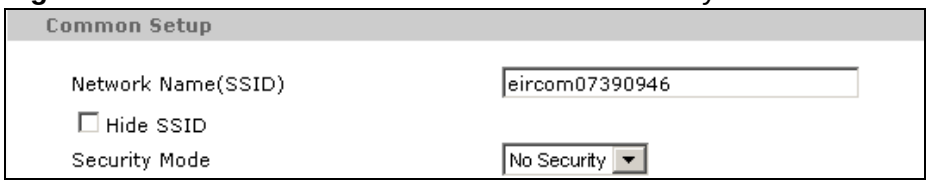
LABEL	DESCRIPTION
QoS	This shows whether Quality of Service (QoS) is activated or the priority level for wireless traffic with this SSID. Select a priority level from the drop-down list box. Choices are **None**, **Default**, **Highest**, **High**, **Middle** and **Low**. Select **None** to disable QoS. Select **Default** to have the ZyXEL Device automatically give traffic a priority level according to the ToS value in the IP header of packets it sends. Wifi MultiMedia Quality of Service (WMM QoS) gives high priority to voice and video, which makes them run more smoothly. **Highest** - Typically used for voice or video that should be high-quality. **High** - Typically used for voice or video that can be medium-quality. **Middle** - Typically used for applications that do not fit into another priority. For example, Internet surfing. **Low** - Typically used for non-critical "background" applications, such as large file transfers and print jobs that should not affect other applications.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced Setup	Click this to display the **Wireless Advanced Setup** screen and edit more details of your WLAN setup. See Section 7.2.5 on page 138 for more details.

7.2.1 No Security

In the **Network > Wireless LAN > AP** screen, select **No Security** from the **Security Mode** list to allow wireless devices to communicate with the ZyXEL Device without any data encryption or authentication.

Note: If you do not enable any wireless security on your ZyXEL Device, your network is accessible to any wireless networking device that is within range.

Figure 30 Network > Wireless LAN > AP: No Security



The following table describes the labels in this screen.

Table 23 Network > Wireless LAN > AP: No Security

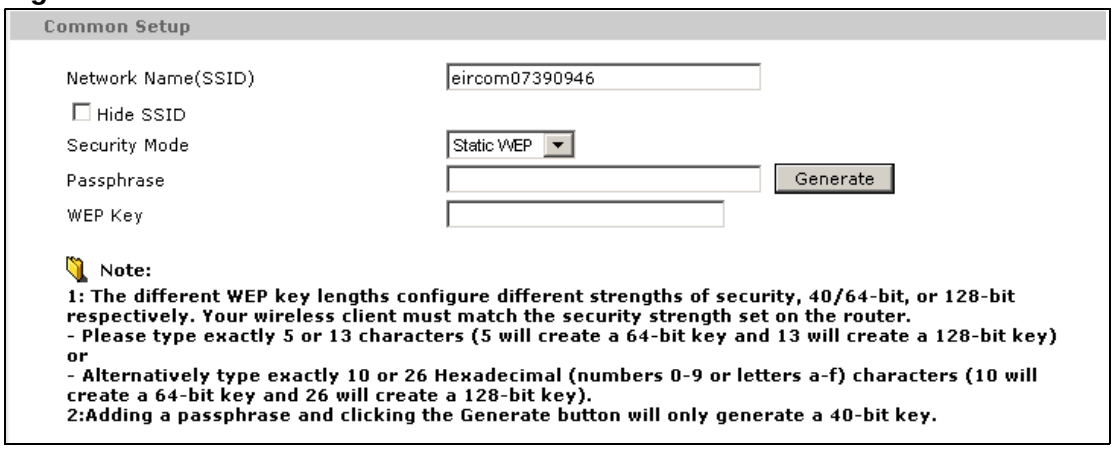
LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.

7.2.2 WEP Encryption

Use this screen to configure and enable WEP encryption. Click **Network > Wireless LAN** to display the **AP** screen. Select **Static WEP** from the **Security Mode** list.

Note: WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. For example, use WPA-PSK or WPA2-PSK if all your wireless devices support it, or use WPA or WPA2 if your wireless devices support it and you have a RADIUS server. If your wireless devices support nothing stronger than WEP, use the highest encryption level available.

Figure 31 Network > Wireless LAN > AP: Static WEP


Common Setup
Network Name(SSID)
eircom07390946
Hide SSID
Security Mode
Static WEP
Passphrase
Generate
WEP Key
Note:
1: The different WEP key lengths configure different strengths of security, 40/64-bit, or 128-bit respectively. Your wireless client must match the security strength set on the router.
- Please type exactly 5 or 13 characters (5 will create a 64-bit key and 13 will create a 128-bit key) or
- Alternatively type exactly 10 or 26 Hexadecimal (numbers 0-9 or letters a-f) characters (10 will create a 64-bit key and 26 will create a 128-bit key).
2:Adding a passphrase and clicking the Generate button will only generate a 40-bit key.

The following table describes the wireless LAN security labels in this screen.

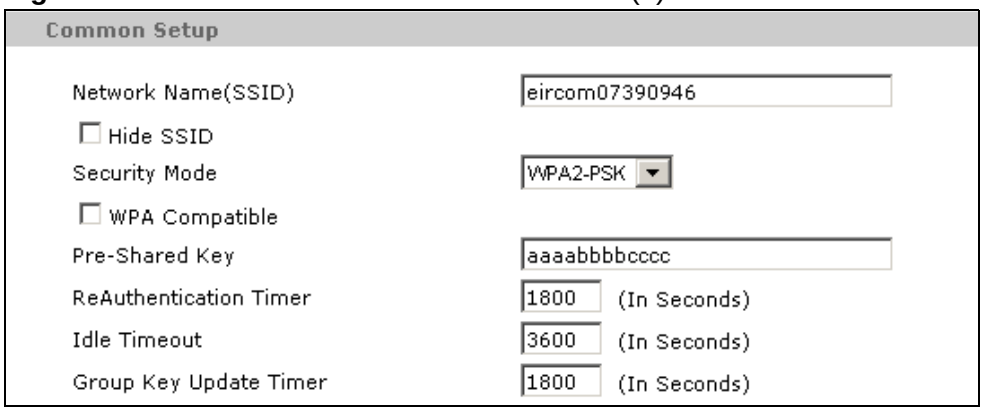
Table 24 Network > Wireless LAN > AP: Static WEP

LABEL	DESCRIPTION
Security Mode	Choose **Static WEP** from the drop-down list box.
Passphrase	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) and click **Generate**. The ZyXEL Device automatically generates a 40-bit WEP key.
WEP Key	The WEP key is used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. If you want to manually set the WEP key, enter any 5 (64-bit) or 13 (128-bit) characters (ASCII string) or 10 or 26 hexadecimal characters ("0-9", lowercase "a-f") for a 64-bit or 128-bit WEP key respectively.

7.2.3 WPA(2)-PSK

Use this screen to configure and enable WPA(2)-PSK authentication. Click **Network > Wireless LAN** to display the **AP** screen. Select **WPA-PSK or WPA2-PSK** from the **Security Mode** list.

Figure 32 Network > Wireless LAN > AP: WPA(2)-PSK



The following table describes the wireless LAN security labels in this screen.

Table 25 Network > Wireless LAN > AP: WPA(2)-PSK

LABEL	DESCRIPTION
Security Mode	Choose **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field. Select the check box to have both WPA-PSK and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
Pre-Shared Key	The encryption mechanisms used for **WPA(2)** and **WPA(2)-PSK** are the same. The only difference between the two is that **WPA(2)-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.

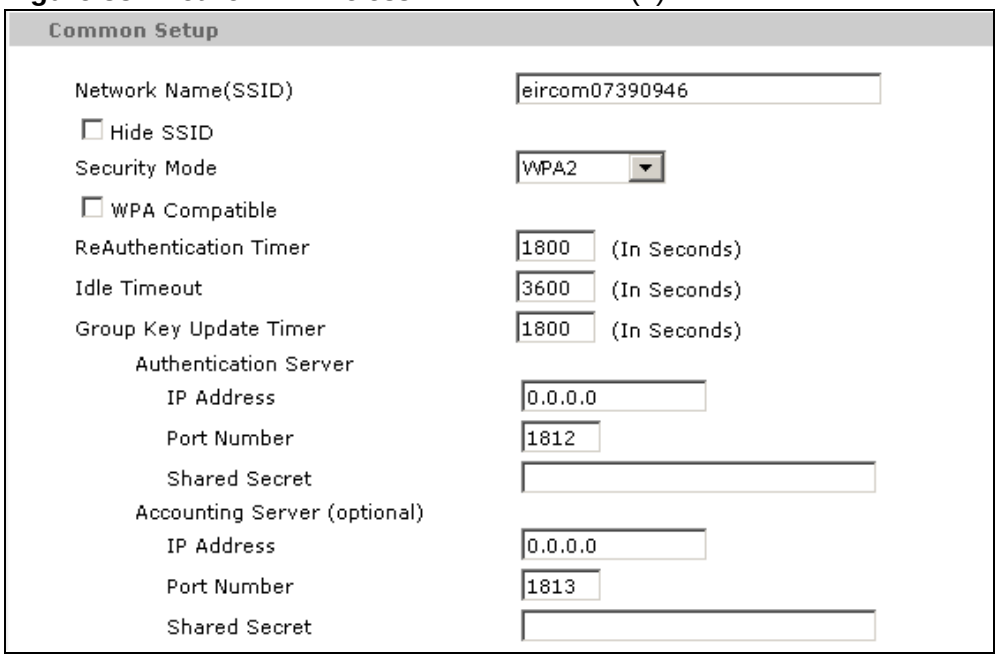
Table 25 Network > Wireless LAN > AP: WPA(2)-PSK

LABEL	DESCRIPTION
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA(2)-PSK** key management) or **RADIUS** server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis.

7.2.4 WPA(2) Authentication

Use this screen to configure and enable WPA or WPA2 authentication. Click the **Wireless LAN** link under **Network** to display the **AP** screen. Select **WPA**, **WPA2** or **WPAMixed** from the **Security Mode** list.

Figure 33 Network > Wireless LAN > AP: WPA(2)



The following table describes the wireless LAN security labels in this screen.

Table 26 Network > Wireless LAN > AP: WPA(2)

LABEL	DESCRIPTION
Security Mode	Choose **WPA** or **WPA2** from the drop-down list box.
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field. Select the check box to have both WPA-PSK and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA(2)-PSK** key management) or **RADIUS** server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
Accounting Server (optional)	
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.

Table 26 Network > Wireless LAN > AP: WPA(2)

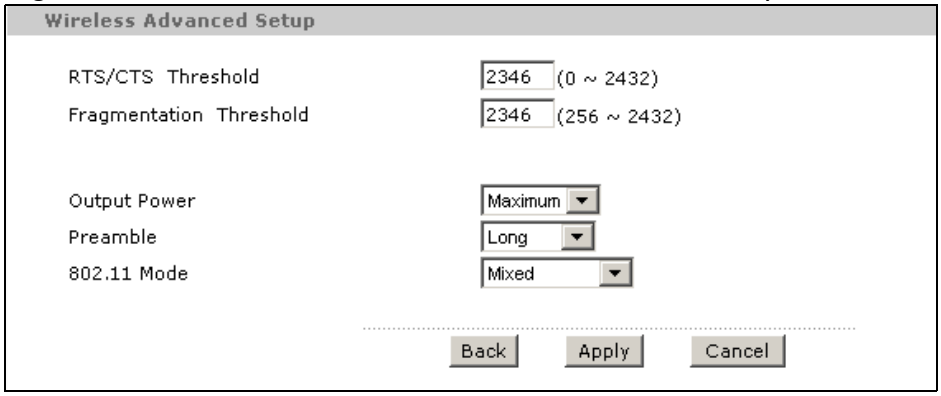
LABEL	DESCRIPTION
Port Number	Enter the port number of the external accounting server. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.

7.2.5 Wireless LAN Advanced Setup

Use this screen to configure advanced wireless settings. Click the **Advanced Setup** button in the **AP** screen. The screen appears as shown.

See Section 7.8.2 on page 149 for detailed definitions of the terms listed in this screen.

Figure 34 Network > Wireless LAN > AP: Advanced Setup



The following table describes the labels in this screen.

Table 27 Network > Wireless LAN > AP: Advanced Setup

LABEL	DESCRIPTION
RTS/CTS Threshold	Enter a value between 0 and 2432.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
Output Power	Set the output power of the ZyXEL Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following **Maximum**, **Middle** or **Minimum**.
Preamble	Select a preamble type from the drop-down list menu. Choices are **Long**, **Short** or **Dynamic**. The default setting is **Long**. See the appendix for more information.

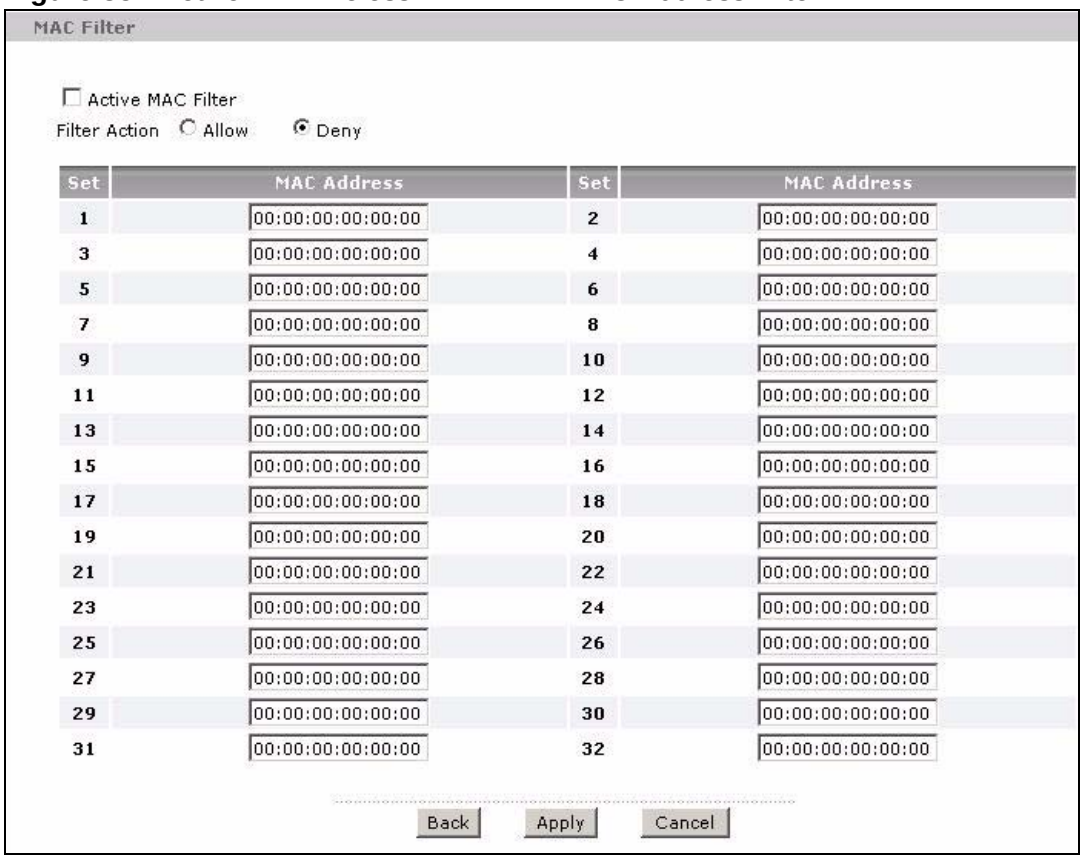
Table 27 Network > Wireless LAN > AP: Advanced Setup

LABEL	DESCRIPTION
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

7.2.6 MAC Filter

Use this screen to change your ZyXEL Device's MAC filter settings. Click the **Edit** button in the **AP** screen. The screen appears as shown.

Figure 35 Network > Wireless LAN > AP: MAC Address Filter



The following table describes the labels in this screen.

Table 28 Network > Wireless LAN > AP: MAC Address Filter

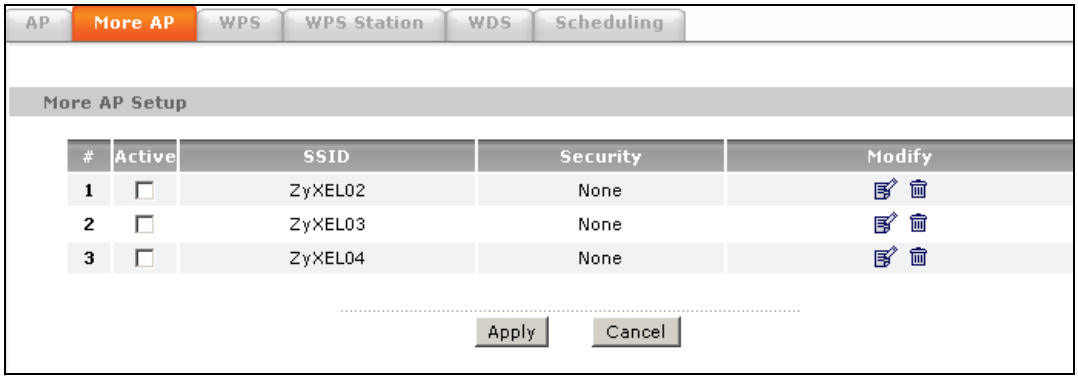
LABEL	DESCRIPTION
Active MAC Filter	Select the check box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny** to block access to the ZyXEL Device. MAC addresses not listed will be allowed to access the ZyXEL Device Select **Allow** to permit access to the ZyXEL Device. MAC addresses not listed will be denied access to the ZyXEL Device.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless devices that are allowed or denied access to the ZyXEL Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

7.3 The More AP Screen

This screen allows you to enable and configure multiple Basic Service Sets (BSSs) on the ZyXEL Device.

Click **Network > Wireless LAN** > **More AP**. The following screen displays.

Figure 36 Network > Wireless LAN > More AP



The following table describes the labels in this screen.

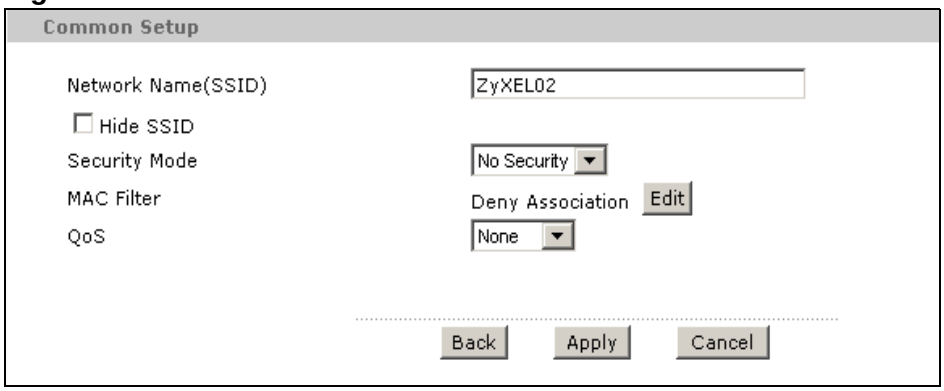
Table 29 Network > Wireless LAN > More AP

LABEL	DESCRIPTION
#	This is the index number of each SSID profile.
Active	Select the check box to activate an SSID profile.
SSID	An SSID profile is the set of parameters relating to one of the ZyXEL Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the **Edit** icon to configure the SSID profile. Click the **Remove** icon to delete the SSID profile.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

7.3.1 More AP Edit

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

Figure 37 Network > Wireless LAN > More AP: Edit



The following table describes the fields in this screen.

Table 30 Network > Wireless LAN > More AP: Edit

LABEL	DESCRIPTION
Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Security Mode	See Section 7.2 on page 131 for more details about this field.
MAC Filter	This shows whether the wireless devices with the MAC addresses listed are allowed or denied to access the ZyXEL Device using this SSID.
Edit	Click this to go to the **MAC Filter** screen to configure MAC filter settings. See Section 7.2.6 on page 139 for more details.
QoS	This shows whether QoS (Quality of Service) is activated or the priority level for wireless traffic with this SSID. Select a priority level from the drop-down list box. Choices are **None**, **Default**, **Highest**, **High**, **Middle** and **Low**. Select **None** to disable QoS. Select **Default** to have the ZyXEL Device automatically give traffic a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. **Highest** - Typically used for voice or video that should be high-quality. **High** - Typically used for voice or video that can be medium-quality. **Middle** - Typically used for applications that do not fit into another priority. For example, Internet surfing. **Low** - Typically used for non-critical "background" applications, such as large file transfers and print jobs that should not affect other applications.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

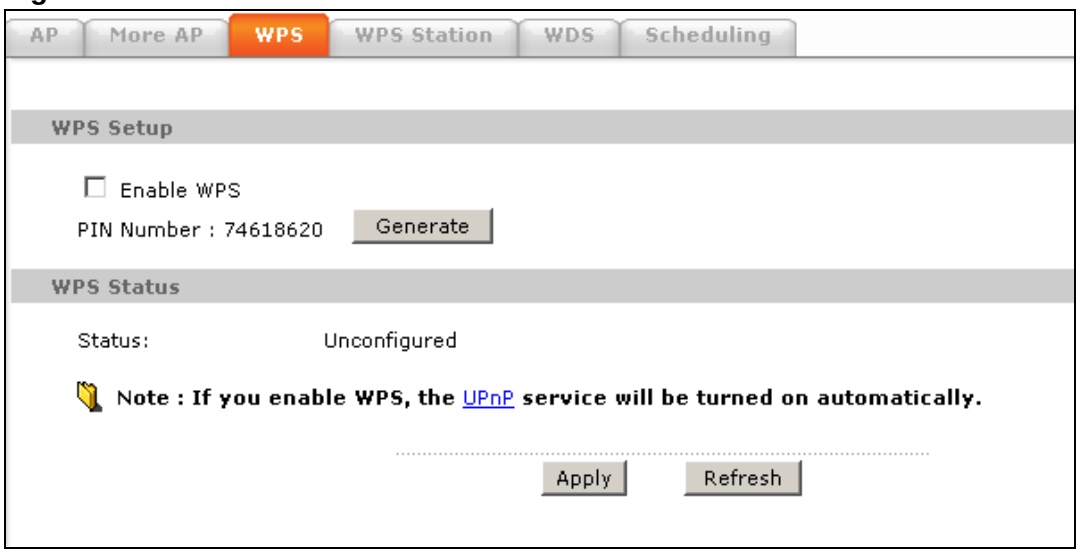
7.4 The WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your ZyXEL Device.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS.

Click **Network > Wireless LAN > WPS**. The following screen displays.

Figure 38 Network > Wireless LAN > WPS



The following table describes the labels in this screen.

Table 31 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select the check box to activate WPS on the ZyXEL Device.
PIN Number	This shows the PIN (Personal Identification Number) of the ZyXEL Device. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method.
Generate	Click this to have the ZyXEL Device create a new PIN.
WPS Status	This displays **Configured** when the ZyXEL Device has connected to a wireless network using WPS or **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there is no wireless or wireless security changes on the ZyXEL Device or you click **Release_Configuration** to remove the configured wireless and wireless security settings.

Table 31 Network > Wireless LAN > WPS

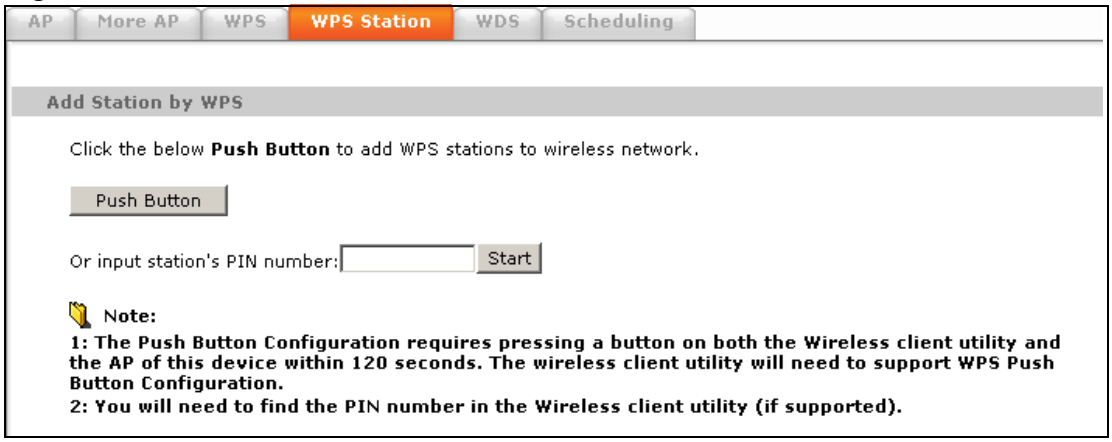
LABEL	DESCRIPTION
Release_Configuration	This button is available when the WPS status is **Configured.** Click this button to remove all configured wireless and wireless security settings for WPS connections on the ZyXEL Device.
Apply	Click this to save your changes.
Refresh	Click this to restore your previously saved settings.

7.5 The WPS Station Screen

Use this screen to set up a WPS wireless network using either Push Button Configuration (PBC) or PIN Configuration.

Click **Network > Wireless LAN > WPS Station**. The following screen displays.

Figure 39 Network > Wireless LAN > WPS Station


AP
More AP
WPS
WPS Station
WDS
Scheduling
Add Station by WPS
Click the below Push Button to add WPS stations to wireless network.
Push Button
Or input station's PIN number:
Start
Note:
1: The Push Button Configuration requires pressing a button on both the Wireless client utility and the AP of this device within 120 seconds. The wireless client utility will need to support WPS Push Button Configuration.
2: You will need to find the PIN number in the Wireless client utility (if supported).

The following table describes the labels in this screen.

Table 32 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Click this to add another WPS-enabled wireless device (within wireless range of the ZyXEL Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **Push Button** on this screen. Note: You must press the other wireless device's WPS button within 120 seconds of pressing this button.
Or input station's PIN number	Enter the PIN of the device that you are setting up a WPS connection with and click **Start** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within 120 seconds to have it present its PIN to the ZyXEL Device.

7.6 The WDS Screen

An AP using the Wireless Distribution System (WDS) can function as a wireless network bridge allowing you to wirelessly connect two wired network segments. The **WDS** screen allows you to configure the ZyXEL Device to connect to two or more APs wirelessly when WDS is enabled.

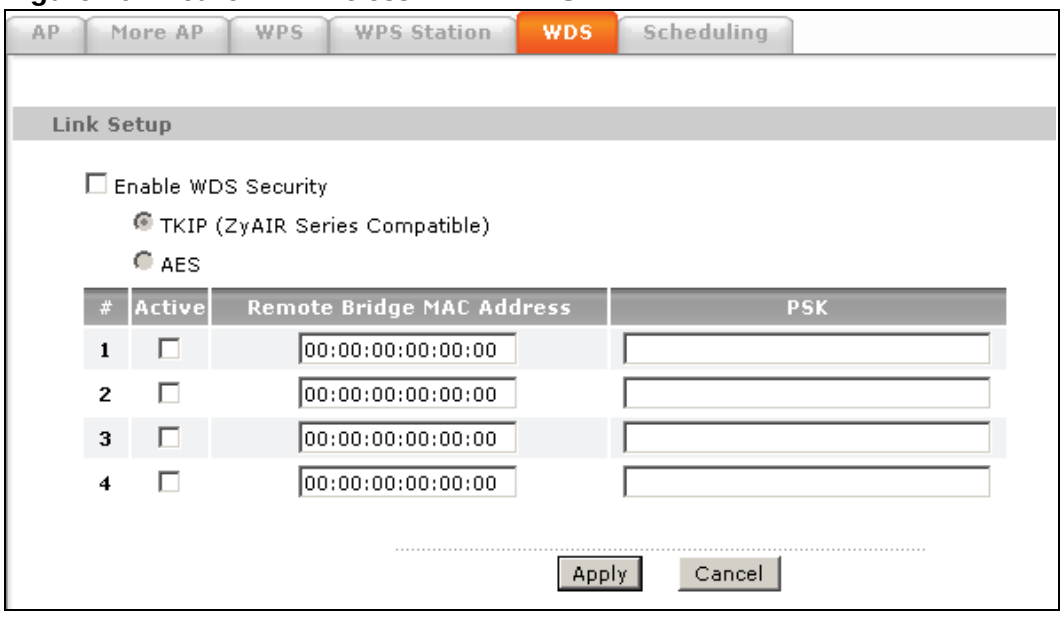
Use this screen to set up your WDS (Wireless Distribution System) links between the ZyXEL Device and other wireless APs. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between devices is made.

Note: WDS security is independent of the security settings between the ZyXEL Device and any wireless clients.

Note: At the time of writing, WDS is compatible with other ZyXEL APs only. Not all models support WDS links. Check your other AP's documentation.

Click **Network > Wireless LAN > WDS**. The following screen displays.

Figure 40 Network > Wireless LAN > WDS



The following table describes the labels in this screen.

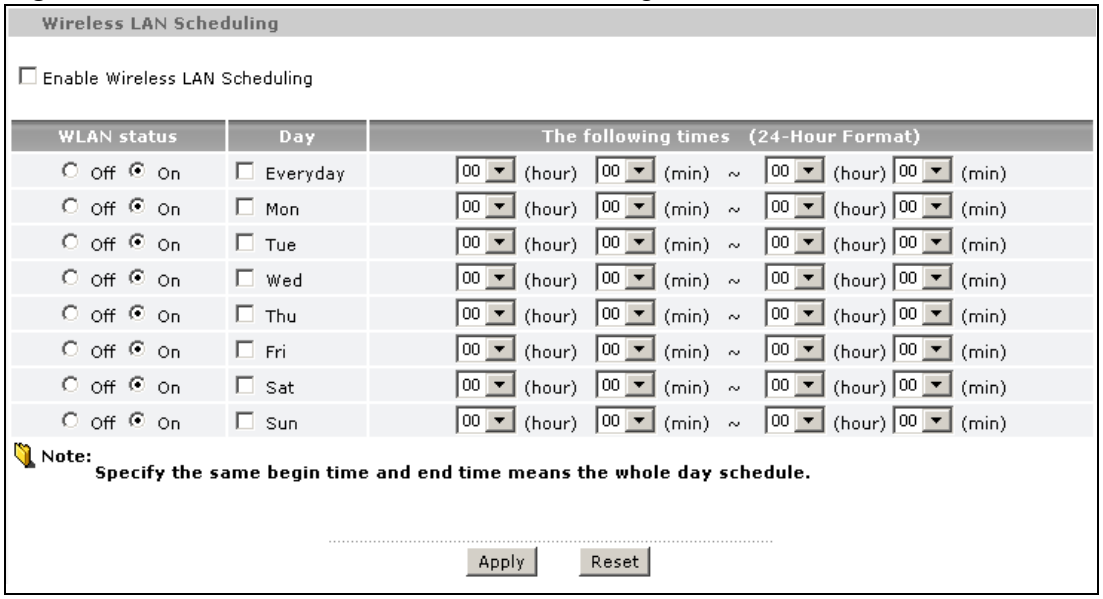
Table 33 Network > Wireless LAN > WDS

LABEL	DESCRIPTION
Enable WDS Security	Select this option and the type of the key used to encrypt data between APs. All the wireless APs (including the ZyXEL Device) must use the same pre-shared key for data transmission. If you de-select this option, the data sent between APs is not encrypted. Anyone can read it.
TKIP	Select this to use TKIP (Temporal Key Integrity Protocol) encryption.
AES	Select this to use AES (Advanced Encryption Standard) encryption.
#	This is the index number of the individual WDS link.
Active	Select this to activate the link between the ZyXEL Device and the peer device to which this entry refers. When you do not select the check box this link is down.
Remote Bridge MAC Address	Type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc).
PSK	Enter a Pre-Shared Key (PSK) from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

7.7 The Scheduling Screen

Use the wireless LAN scheduling to configure the days you want to enable or disable the wireless LAN. Click **Network > Wireless LAN > Scheduling**. The following screen displays.

Figure 41 Network > Wireless LAN > Scheduling



The following table describes the labels in this screen.

Table 34 Network > Wireless LAN > Scheduling

LABEL	DESCRIPTION
Enable Wireless LAN Scheduling	Select this box to activate wireless LAN scheduling on your ZyXEL Device.
WLAN status	Select **On** or **Off** to enable or disable the wireless LAN.
Day	Check the day(s) you want to turn the wireless LAN on or off.
The following times	Specify a time frame during which the schedule would apply. For example, if you set the time range from 12:00 to 23:00, the wireless LAN will be turned on only during this time period.
Apply	Click this to save your changes.
Reset	Click this to restore your previously saved settings.

7.8 Wireless LAN Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

7.8.1 Wireless Network Overview

Wireless networks consist of wireless clients, access points and bridges.

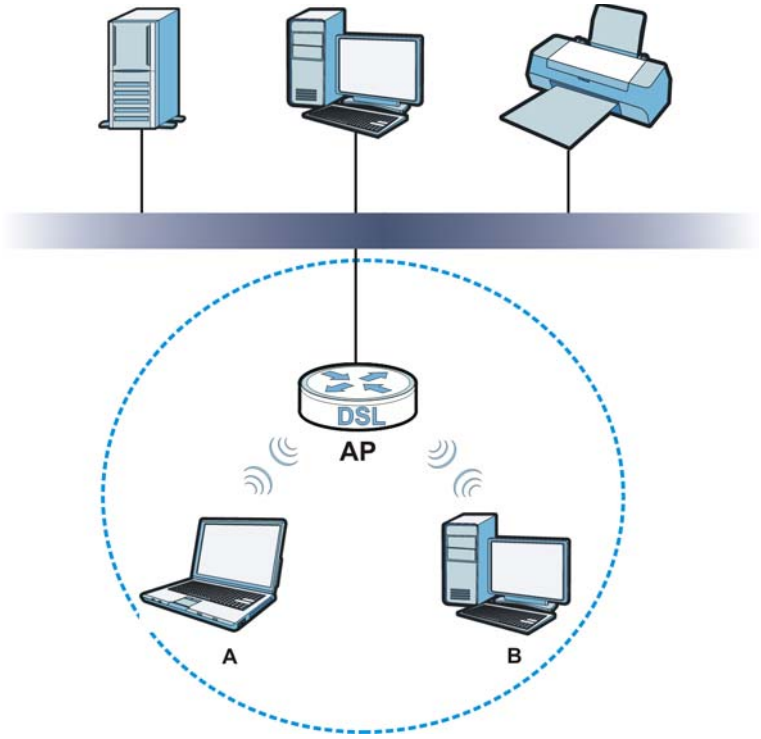
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 42 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your ZyXEL Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentifier.

- If two wireless networks overlap, they should use a different channel.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every device in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

7.8.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the ZyXEL Device's Web Configurator.

Table 35 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the ZyXEL Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the ZyXEL Device.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the ZyXEL Device does, it cannot communicate with the ZyXEL Device.

Table 35 Additional Wireless Terms

TERM	DESCRIPTION
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

7.8.3 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a “key” phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker’s software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it’s not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point

(which you know was made in 1971) you could use “70dodchal71vanpoi” as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

7.8.3.1 SSID

Normally, the ZyXEL Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the ZyXEL Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

7.8.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device’s User’s Guide or other documentation.

You can use the MAC address filter to tell the ZyXEL Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

7.8.3.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

7.8.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See Section 7.8.3.3 on page 151 for information about this.)

Table 36 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
↕	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the ZyXEL Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your ZyXEL Device, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the

devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the ZyXEL Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

7.8.4 Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

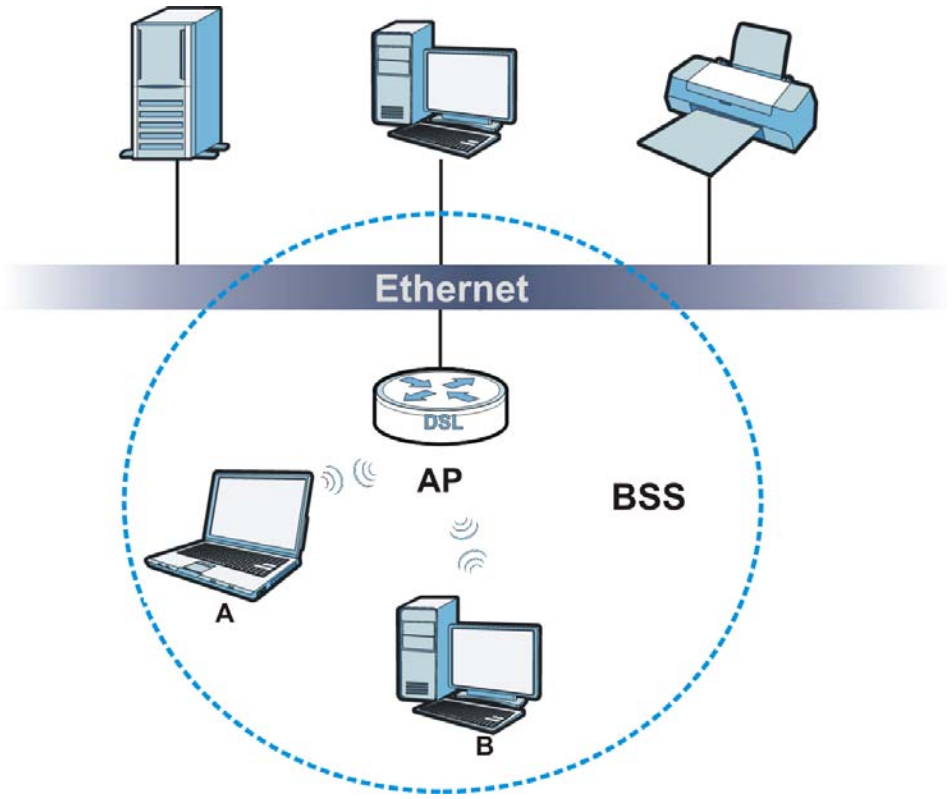
7.8.5 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled,

wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 43 Basic Service set



7.8.6 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The ZyXEL Device's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

7.8.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

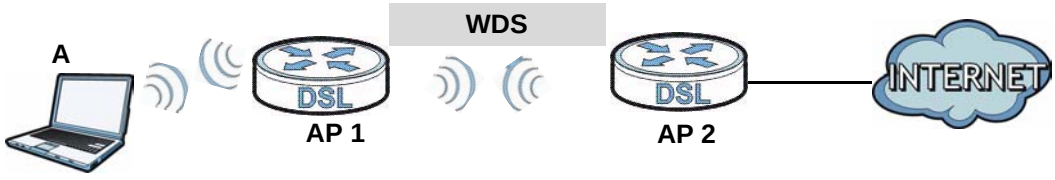
7.8.7 Wireless Distribution System (WDS)

The ZyXEL Device can act as a wireless network bridge and establish WDS (Wireless Distribution System) links with other APs. You need to know the MAC addresses of the APs you want to link to. Once the security settings of peer sides match one another, the connection between devices is made.

At the time of writing, WDS security is compatible with other ZyXEL access points only. Refer to your other access point's documentation for details.

The following figure illustrates how WDS link works between APs. Notebook computer **A** is a wireless client connecting to access point **AP 1**. **AP 1** has no wired Internet connection, but it can establish a WDS link with access point **AP 2**, which has a wired Internet connection. When **AP 1** has a WDS link with **AP 2**, the notebook computer can access the Internet through **AP 2**.

Figure 44 WDS Link Example



7.8.8 WiFi Protected Setup (WPS)

Your ZyXEL Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

7.8.8.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the ZyXEL Device, see Section 7.5 on page 144).
3. Press the button on one of the devices (it doesn't matter which). For the ZyXEL Device, the wireless LAN is activated by default, so the LED lights green. If not, press the WIFI button for 5 to 6 seconds and release it when the LED turns green. The Wireless LAN is on. Press the WIFI button again for 1 to 2 seconds and release it when the LED is blinking orange. Press the WiFi or WPS button on another WPS-enabled device within range of the ZyXEL Device.
4. Within two minutes, press the button on the other device. The **WiFi** LED blinks orange while the registrar sends the network name (SSID) and security key through an secure connection to the enrollee. When the WPS connection has been configured successfully, the LED will become green.

   If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

7.8.8.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

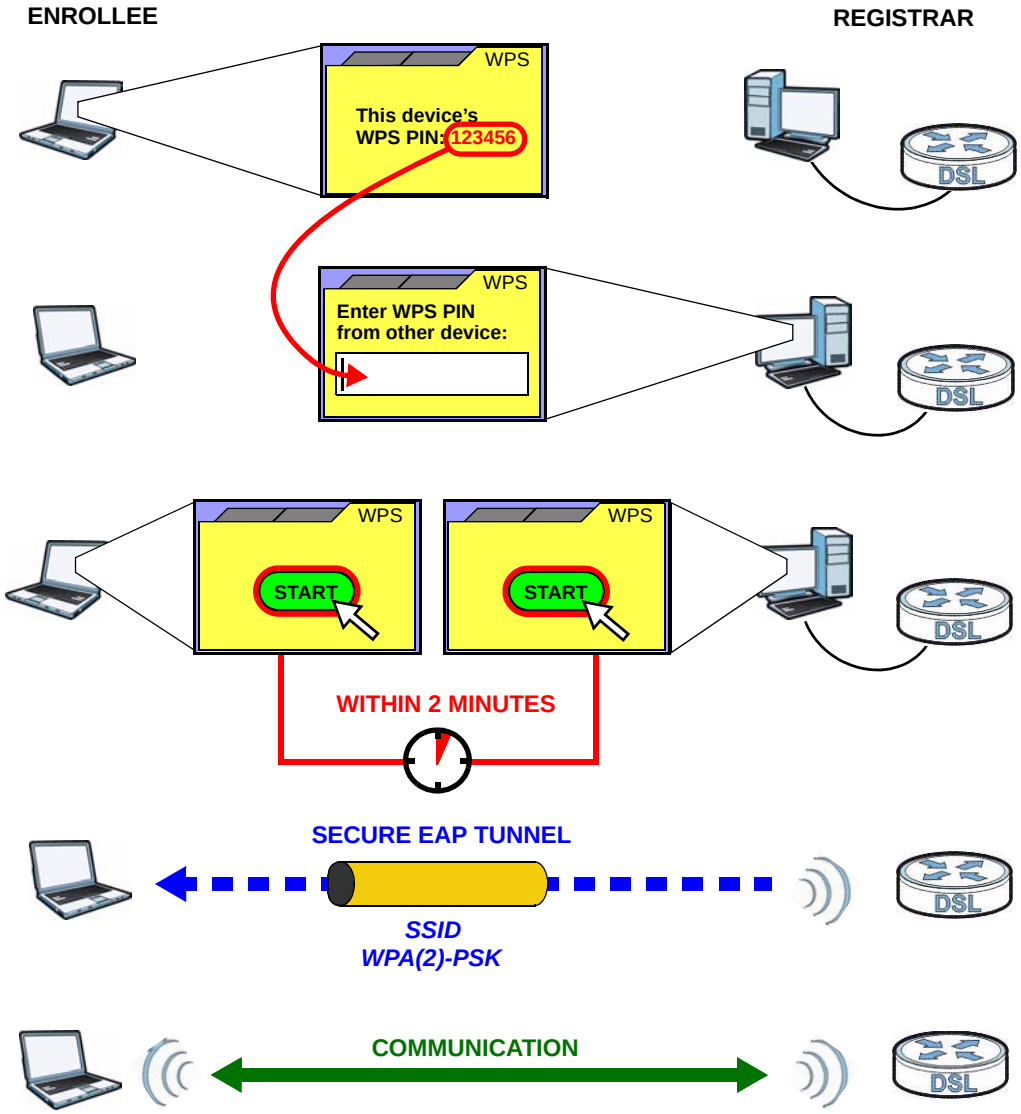
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

1. Ensure WPS is enabled on both devices.
2. Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
3. Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the ZyXEL Device, see Section 7.4 on page 143).
4. Enter the client's PIN in the AP's configuration interface.
5. If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
6. Start WPS on both devices within two minutes.
7. Use the configuration utility to activate WPS, not the push-button on the device itself.
8. On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

   If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 45 Example WPS Process: PIN Method

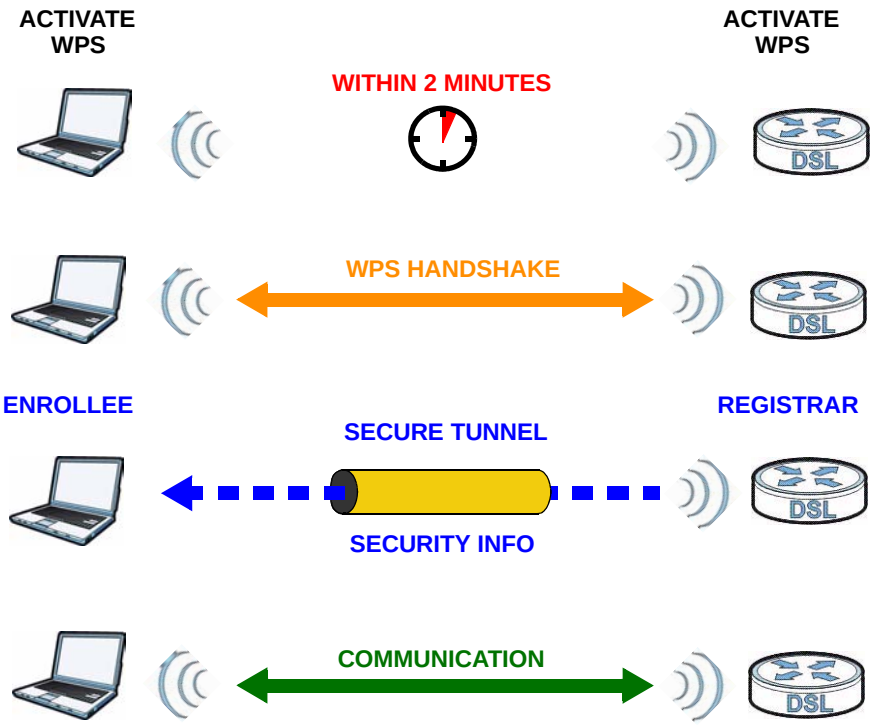


7.8.8.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 46 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

7.8.8.4 Example WPS Network Setup

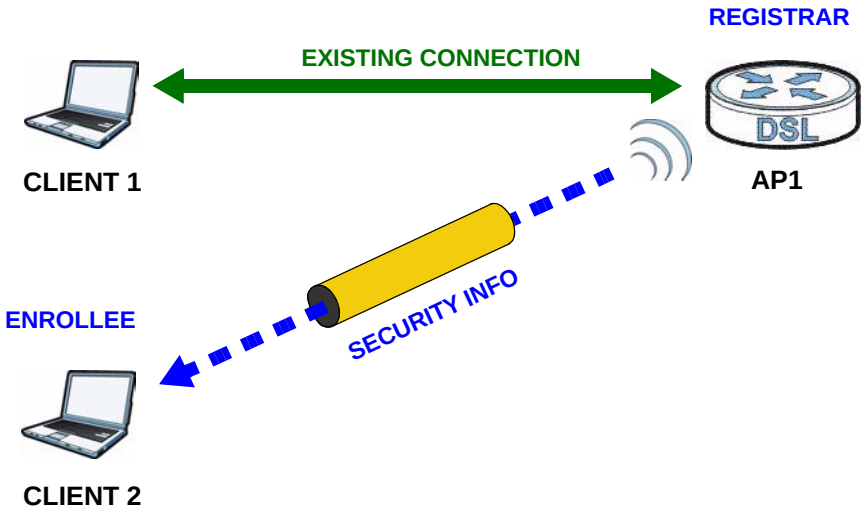
This section shows how security settings are distributed in an example WPS setup.

The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 47 WPS: Example Network Step 1

In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

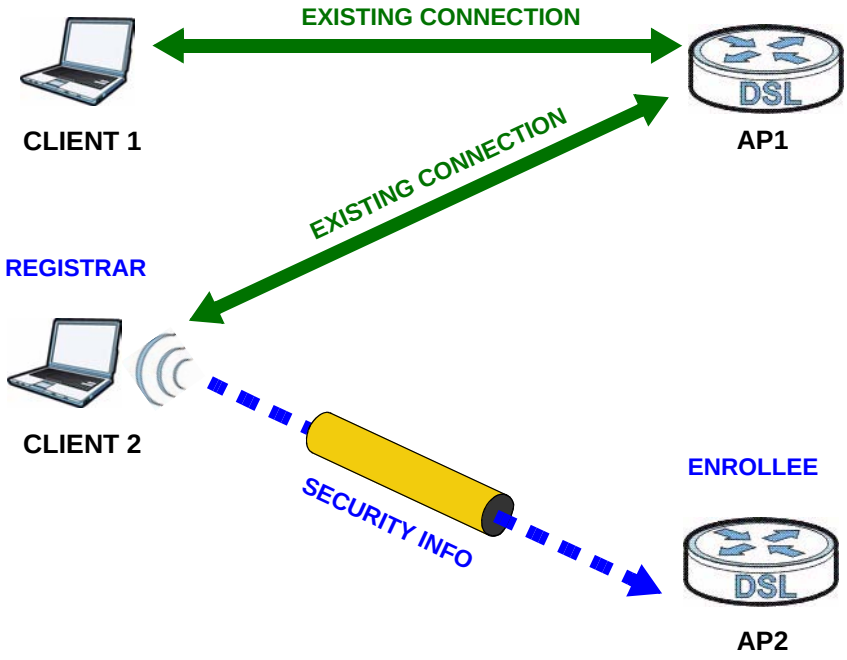
Figure 48 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access

point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 49 WPS: Example Network Step 3



7.8.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

8

Network Address Translation (NAT)

8.1 Overview

This chapter discusses how to configure NAT on the ZyXEL Device. NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

8.1.1 What You Can Do in the NAT Screens

- Use the **NAT General Setup** screen (Section 8.2 on page 165) to configure the NAT setup settings.
- Use the **Port Forwarding** screen (Section 8.3 on page 166) to configure forward incoming service requests to the server(s) on your local network.
- Use the **Address Mapping** screen (Section 8.4 on page 169) to change your ZyXEL Device's address mapping settings.
- Use the **ALG** screen (Section 8.5 on page 173) to enable and disable the SIP (VoIP) ALG in the ZyXEL Device.

8.1.2 What You Need To Know About NAT

Inside/Outside

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in Table 44 on page 177.

- Choose **SUA Only** if you have just one public WAN IP address for your ZyXEL Device.
- Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyXEL Device.

Finding Out More

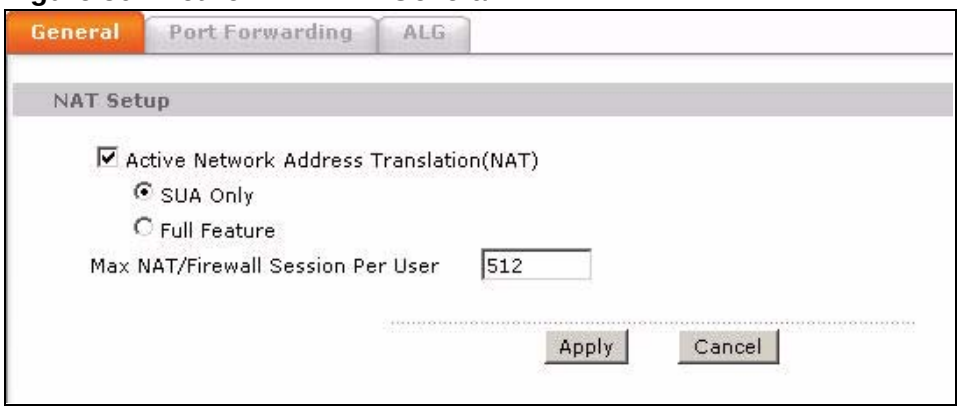
See Section 8.6 on page 173 for advanced technical information on NAT.

8.2 The NAT General Setup Screen

Use this screen to activate NAT. Click **Network > NAT** to open the following screen.

Note: You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyXEL Device.

Figure 50 Network > NAT > General



The following table describes the labels in this screen.

Table 37 Network > NAT > General

LABEL	DESCRIPTION
Active Network Address Translation (NAT)	Select this check box to enable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your ZyXEL Device.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your ZyXEL Device.
Max NAT/ Firewall Session Per User	When computers use peer to peer applications, such as file sharing applications, they need to establish NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet. Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/Firewall sessions client computers can establish through the ZyXEL Device. If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is exhausting all of the available NAT sessions.

Table 37 Network > NAT > General (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

8.3 The Port Forwarding Screen

Use this screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

The most often used port numbers and services are shown in Appendix E on page 421. Please refer to RFC 1700 for further information about port numbers.

Note: This screen is available only when you select **SUA only** in the **NAT > General** screen.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Note: When using the port forwarding feature, make sure your firewall is configured as **Low**, **Custom**, or **Off**.

Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

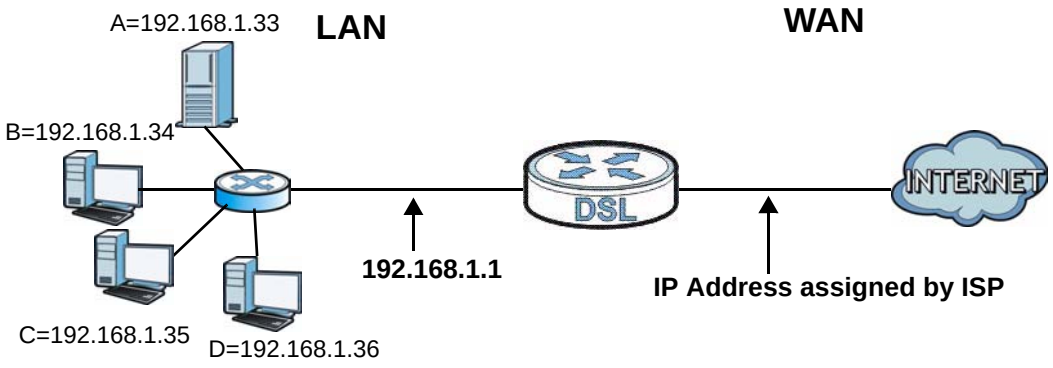
Note: If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

Note: Setting a device as the default server exposes the device to potential attacks. Any port service trying to access the ZyXEL Device's WAN IP address will be forwarded to the default server. It is recommended that you set up a firewall rule to protect the device.

Configuring Servers Behind Port Forwarding

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 51 Multiple Servers Behind NAT



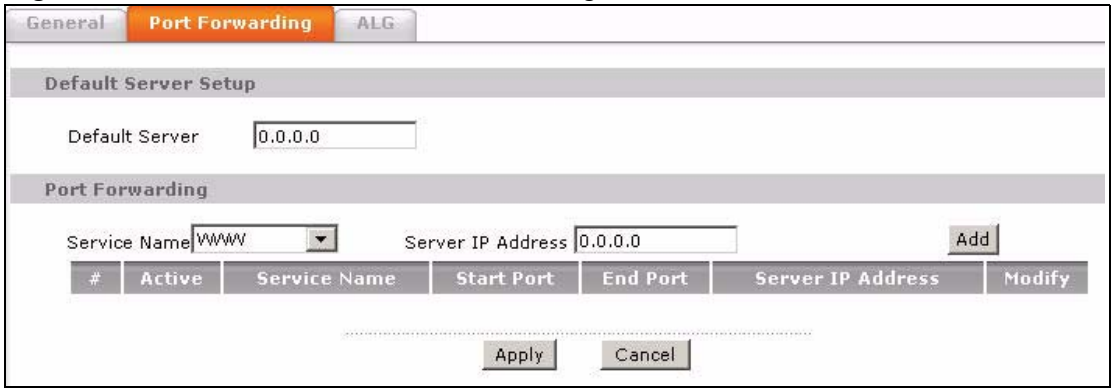
8.3.1 Configuring the Port Forwarding Screen

Click **Network > NAT > Port Forwarding** to open the following screen.

Note: If WAN IP Passthrough is activated, Port Forwarding will be disabled.

See Appendix E on page 421 for port numbers commonly used for particular services.

Figure 52 Network > NAT > Port Forwarding



The following table describes the fields in this screen.

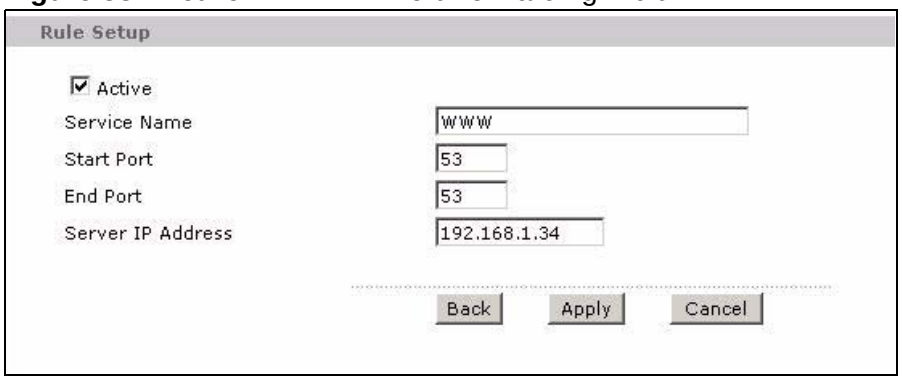
Table 38 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.
Port Forwarding	
Service Name	Select a service from the drop-down list box.
Server IP Address	Enter the IP address of the server for the specified service.
Add	Click this button to add a rule to the table below.
#	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Service Name	This is a service's name.
Start Port	This is the first port number that identifies a service.
End Port	This is the last port number that identifies a service.
Server IP Address	This is the server's IP address.
Modify	Click the edit icon to go to the screen where you can edit the port forwarding rule. Click the delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

8.3.2 The Port Forwarding Rule Edit Screen

Use this screen to edit a port forwarding rule. Click the rule's edit icon in the **Port Forwarding** screen to display the screen shown next.

Figure 53 Network > NAT > Port Forwarding: Edit



The following table describes the fields in this screen.

Table 39 Network > NAT > Port Forwarding: Edit

LABEL	DESCRIPTION
Active	Click this check box to enable the rule.
Service Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number in this field. To forward only one port, enter the port number again in the **End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port** field.
End Port	Enter a port number in this field. To forward only one port, enter the port number again in the **Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port** field above.
Server IP Address	Enter the inside IP address of the server here.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

8.4 The Address Mapping Screen

Ordering your rules is important because the ZyXEL Device applies the rules in the order that you specify. When a rule matches the current packet, the ZyXEL Device

takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

Note: The **Address Mapping** screen is available only when you select **Full Feature** in the **NAT > General** screen.

To change your ZyXEL Device's address mapping settings, click **Network > NAT > Address Mapping** to open the following screen.

Figure 54 Network > NAT > Address Mapping

General
Address Mapping
ALG
Address Mapping Rules
Local Start IP Local End IP Global Start IP Global End IP Type Modify
1 - - - - -
2 - - - - -
3 - - - - -
4 - - - - -
5 - - - - -
6 - - - - -
7 - - - - -
8 - - - - -
9 - - - - -
10 - - - - -

The following table describes the fields in this screen.

Table 40 Network > NAT > Address Mapping

LABEL	DESCRIPTION
#	This is the rule index number.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-one** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-one**, **Many-to-One** and **Server** mapping types.

Table 40 Network > NAT > Address Mapping (continued)

LABEL	DESCRIPTION
Type	**1-1**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **M-1**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. **M-M Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. **MM No** (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Modify	Click the edit icon to go to the screen where you can edit the address mapping rule. Click the delete icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

8.4.1 The Address Mapping Rule Edit Screen

Use this screen to edit an address mapping rule. Click the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

Figure 55 Network > NAT > Address Mapping: Edit

The following table describes the fields in this screen.

Table 41 Network > NAT > Address Mapping: Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. **Many-to-Many No Overload**: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Server Mapping Set	Only available when **Type** is set to **Server**. Select a number from the drop-down menu to choose a port forwarding set.
Edit Details	Click this link to go to the **Port Forwarding** screen to edit a port forwarding set that you have selected in the **Server Mapping Set** field.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

8.5 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the ZyXEL Device registers with the SIP register server, the SIP ALG translates the ZyXEL Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your ZyXEL Device is behind a SIP ALG.

Use this screen to enable and disable the SIP (VoIP) ALG in the ZyXEL Device. To access this screen, click **Network > NAT > ALG**.

Figure 56 Network > NAT > ALG

The following table describes the fields in this screen.

Table 42 Network > NAT > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Select this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
Apply	Click this to save your changes.
Reset	Click this to restore your previously saved settings.

8.6 NAT Technical Reference

This chapter contains more information regarding NAT.

8.6.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the

packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 43 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

8.6.2 What NAT Does

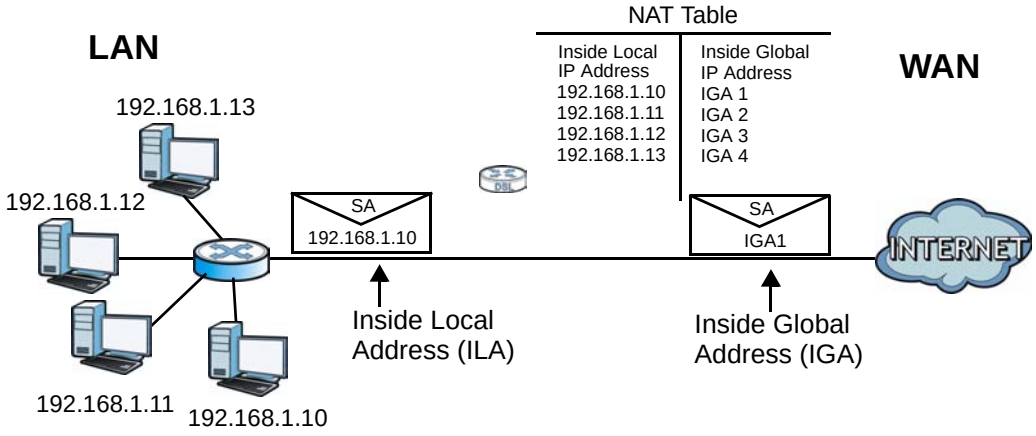
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see Table 44 on page 177), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

8.6.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyXEL Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

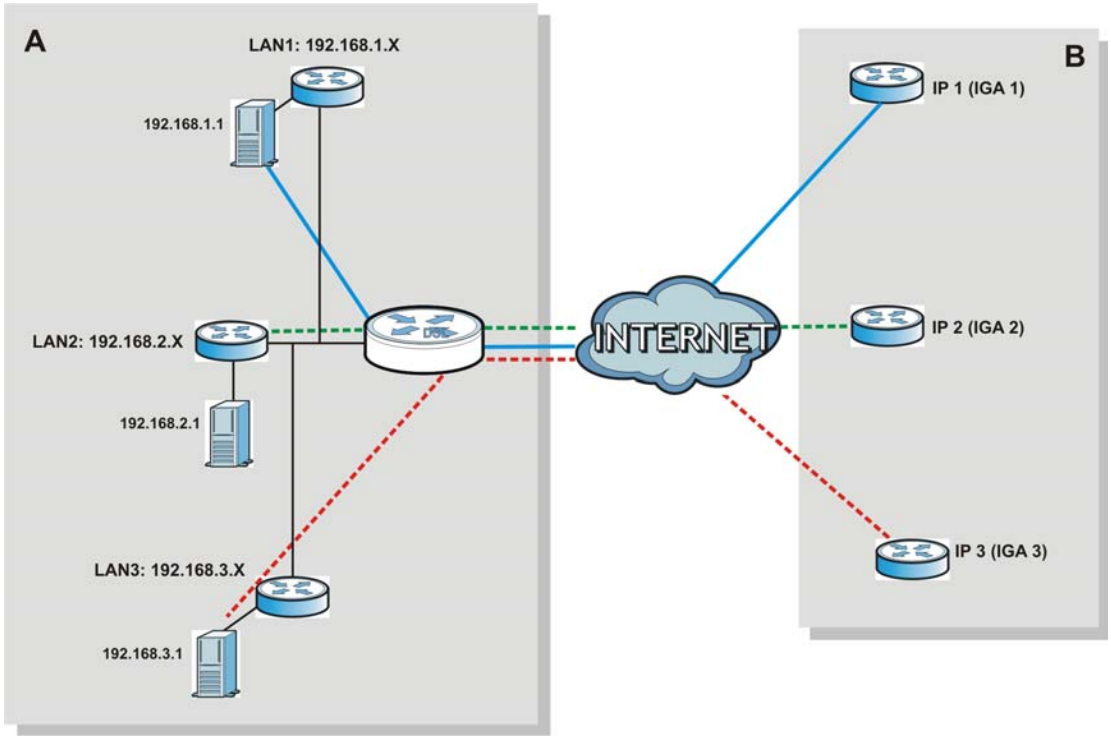
Figure 57 How NAT Works



8.6.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the ZyXEL Device can communicate with three distinct WAN networks.

Figure 58 NAT Application With IP Alias



8.6.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the ZyXEL Device maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the ZyXEL Device maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
- **Many to Many Overload**: In Many-to-Many Overload mode, the ZyXEL Device maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload**: In Many-to-Many No Overload mode, the ZyXEL Device maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do NOT change for **One-to-One** and **Many-to-Many No Overload** NAT mapping types.

The following table summarizes these types.

Table 44 NAT Mapping Types

TYPE	IP MAPPING
One-to-One	ILA1←→ IGA1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 ...
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 ...
Many-to-Many No Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 ...
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1

PART III
Security

Firewalls (181)

Content Filtering (205)

Packet Filter (211)

Certificates (223)

9

Firewalls

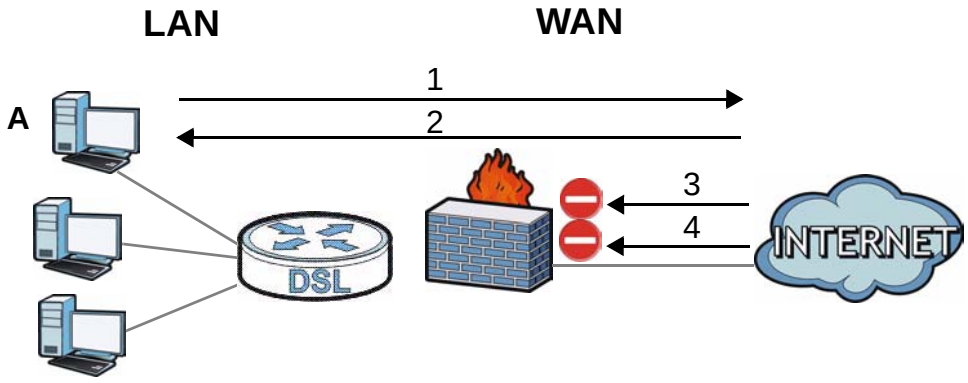
9.1 Overview

This chapter shows you how to enable and configure the ZyXEL Device firewall. Use these screens to enable and configure the firewall that protects your ZyXEL Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 59 Default Firewall Action



9.1.1 What You Can Do in the Firewall Screens

- Use the **General** screen (Section 9.2 on page 186) to enable firewall or set the firewall level on the ZyXEL Device.
- Use the **Rules** screen (Section 9.3 on page 189) to view the configured firewall rules and add, edit or remove a firewall rule when you set the firewall level as **Custom** in the **General** screen.

- Use the **Threshold** screen (Section 9.4 on page 197) to set the thresholds that the ZyXEL Device uses to determine when to start dropping sessions that do not become fully established (half-open sessions).

9.1.2 What You Need to Know About Firewall

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

Anti-Probing

If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. The ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

DoS Thresholds

For DoS attacks, the ZyXEL Device uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions. You can use the default threshold values, or you can change them to values more suitable to your security requirements.

Finding Out More

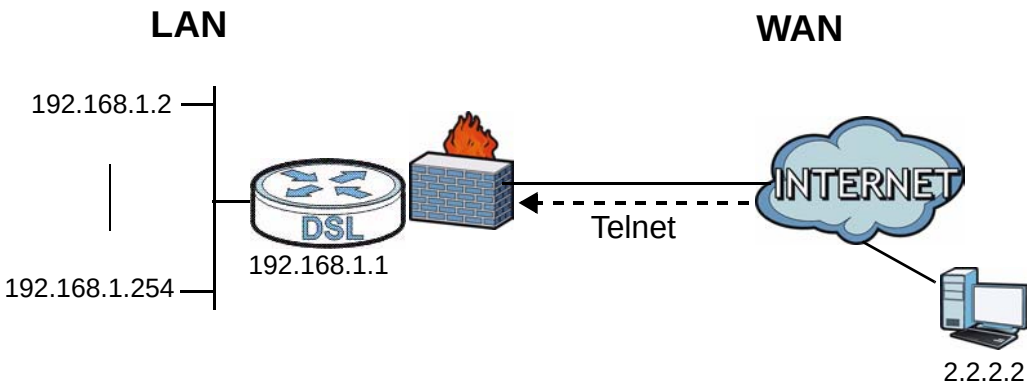
- See Section 9.1.3 on page 182 for an example of setting up a firewall.
- See Section 9.5 on page 200 for advanced technical information on firewall.

9.1.3 Firewall Rule for WAN Telnet Connection Example

The following Internet firewall rule example allows a Telnet connection from the Internet. You must also configure remote management to allow Telnet from the

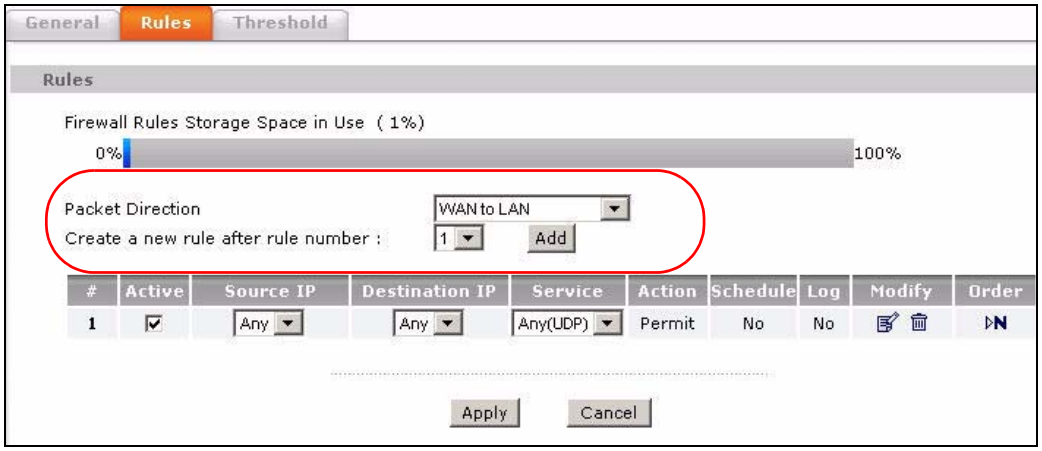
WAN. See **Advanced > Remote MGMT** > **Telnet** (Section 18.3 on page 284) for more information.

Figure 60 Firewall Rule Setup for Telnet Connection



1 Select **Custom** from the **General** screen. The **Rules** tab will appear. Click the tab to go to **Rules** screen.

2 Select **WAN to LAN** in the **Packet Direction** field.



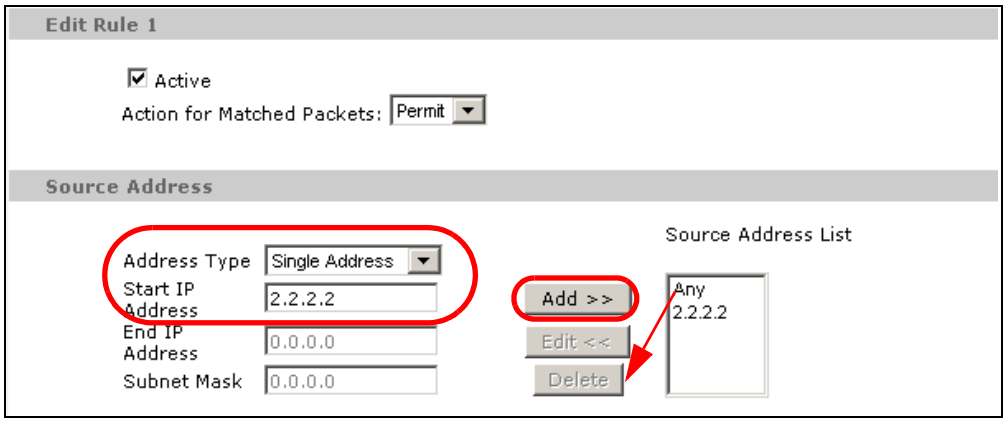
3 In the **Rules** screen, select the index number after that you want to add the rule.

4 Click **Add** to display the firewall rule configuration screen.

5 Select **Single Address** from the **Address Type** drop list of **Source Address**.

6 Enter the IP address of the computer from which you want to allow Telnet (2.2.2.2) into the **Start IP Address** field. The IP address must be in dotted decimal notation. Then click **Add**.

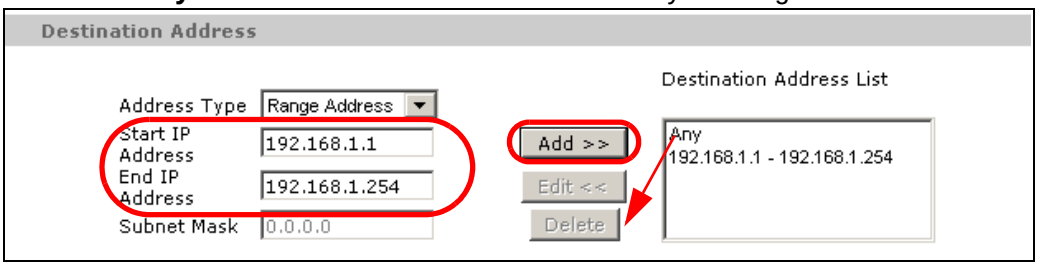
7 Delete **Any** in the **Source Address List** box by clicking **Delete**.



8 Select **Range Address** from the **Address Type** drop list of **Destination Address**.

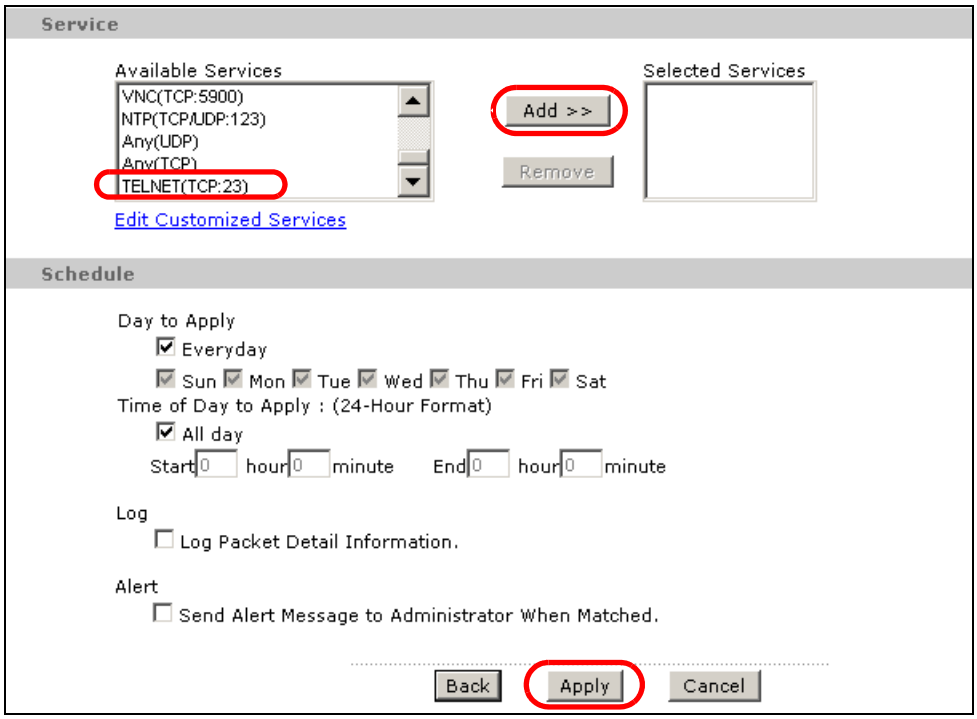
9 Enter the IP address range of the ZyXEL Device (192.168.1.1) and computers on your network (192.168.1.2 - 192.168.1.254) into the **Start IP Address** and **End IP Address** fields. The IP addresses must be in dotted decimal notation. Then click **Add**.

10 Delete **Any** in the **Source Address List** box by clicking **Delete**.



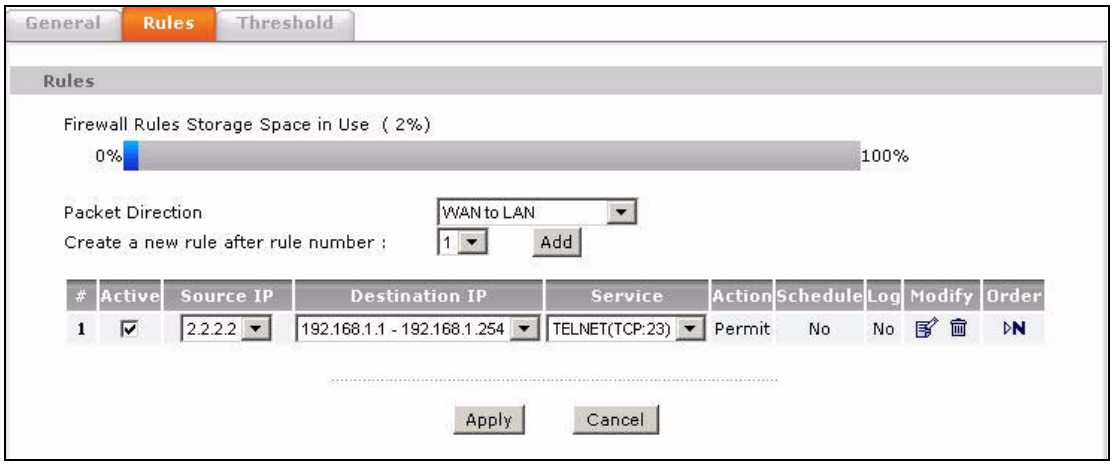
11 Select **TELNET(TCP:23)** from the **Available Service** list. Use the **Add >>** button to add it to the **Selected Services** list. Use the **Remove** button to remove services you do not need.

12 Configure other settings in **Schedule**. Click **Apply** when you are done.



On completing the configuration procedure, the **Rules** screen should look like the following.

The firewall rule allows a Telnet connection from WAN IP 2.2.2.2 to IP addresses 192.168.1.1 through 192.168.1.254.



9.2 The Firewall General Screen

9.2.1 Firewall Rules Overview

Your customized rules take precedence and override the ZyXEL Device's default settings. The ZyXEL Device checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ZyXEL Device takes the action specified in the rule.

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to LAN/ Router
- LAN to WAN
- WAN to LAN
- WAN to WAN/ Router

Note: The LAN includes both the LAN port and the WLAN.

By default, the ZyXEL Device's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ Router

  These rules specify which computers on the LAN can manage the ZyXEL Device (remote management) and communicate between networks or subnets connected to the LAN interface (IP alias).

Note: You can also configure the remote management settings to allow only a specific computer to manage the ZyXEL Device.

- LAN to WAN

  These rules specify which computers on the LAN can access which computers or services on the WAN.

By default, the ZyXEL Device's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN

  These rules specify which computers on the WAN can access which computers or services on the LAN.

Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN.

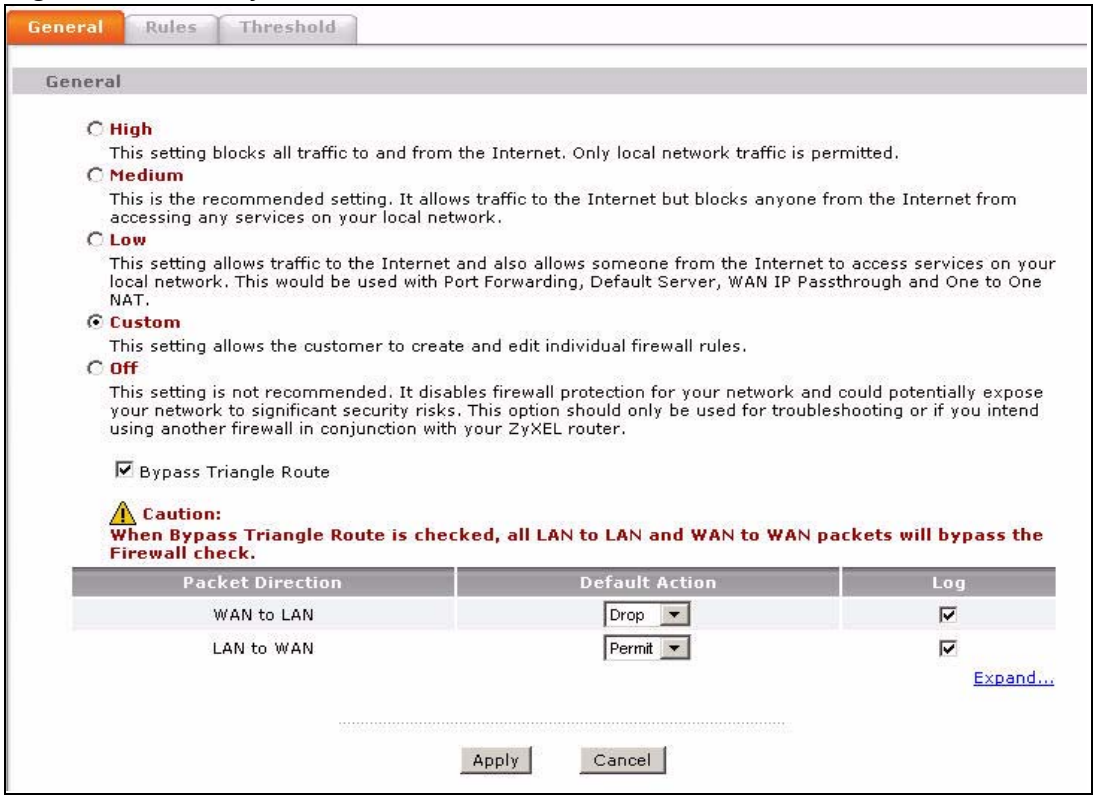
- WAN to WAN/ Router

  By default the ZyXEL Device stops computers on the WAN from managing the ZyXEL Device or using the ZyXEL Device as a gateway to communicate with other computers on the WAN. You could configure one of these rules to allow a WAN computer to manage the ZyXEL Device.

You need to configure the remote management settings to allow a WAN computer to manage the ZyXEL Device.

Use this screen to configure the firewall settings. Click **Security > Firewall** to display the following screen.

Figure 61 Security > Firewall > General


General
Rules
Threshold
General
High
This setting blocks all traffic to and from the Internet. Only local network traffic is permitted.
Medium
This is the recommended setting. It allows traffic to the Internet but blocks anyone from the Internet from accessing any services on your local network.
Low
This setting allows traffic to the Internet and also allows someone from the Internet to access services on your local network. This would be used with Port Forwarding, Default Server, WAN IP Passthrough and One to One NAT.
Custom
This setting allows the customer to create and edit individual firewall rules.
Off
This setting is not recommended. It disables firewall protection for your network and could potentially expose your network to significant security risks. This option should only be used for troubleshooting or if you intend using another firewall in conjunction with your ZyXEL router.
Bypass Triangle Route
Caution:
When Bypass Triangle Route is checked, all LAN to LAN and WAN to WAN packets will bypass the Firewall check.
Packet Direction
Default Action
Log
WAN to LAN
Drop
LAN to WAN
Permit
Expand...
Apply
Cancel

The following table describes the labels in this screen.

Table 45 Security > Firewall > General

LABEL	DESCRIPTION
High	Select this to turn off all traffic to and from the Internet. Only traffic within your local network (LAN to LAN) is allowed.
Medium	Select this to allow traffic to the Internet but disallow traffic from the Internet to your local network. This permits LAN to LAN and LAN to WAN traffic.

Table 45 Security > Firewall > General

LABEL	DESCRIPTION
Low	Select this to allow traffic to the Internet and allow Internet access to your local network from those WAN computers for which you configured Port Forwarding, Default Server, WAN IP Passthrough, and One to One NAT. This permits LAN to LAN, LAN to WAN, and WAN to LAN (with NAT configured).
Custom	Select this to create and edit your own firewall rules. You can do this in the **Rules** screen, which appears when you choose **Custom**.
Off	Select this disable all firewall protection. This allows all traffic to and from the Internet to your ZyXEL Device.
Bypass Triangle Route	If an alternate gateway on the LAN has an IP address in the same subnet as the ZyXEL Device's LAN IP address, return traffic may not go through the ZyXEL Device. This is called an asymmetrical or "triangle" route. This causes the ZyXEL Device to reset the connection, as the connection has not been acknowledged. Select this check box to have the ZyXEL Device permit the use of asymmetrical route topology on the network (not reset the connection). Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyXEL Device. A better solution is to use IP alias to put the ZyXEL Device and the backup gateway on separate subnets. See Section 9.5.3.2 on page 203 for an example.
Packet Direction	This is the direction of travel of packets (**LAN to LAN / Router**, **LAN to WAN**, **WAN to WAN / Router**, **WAN to LAN)**. Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, **LAN to LAN / Router** means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the ZyXEL Device or the ZyXEL Device itself.
Default Action	Use the drop-down list boxes to select the default action that the firewall is to take on packets that are traveling in the selected direction and do not match any of the firewall rules. Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select **Permit** to allow the passage of the packets.
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of your customized rules.
Expand...	Click this to display more information.
Basic...	Click this to display less information.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

9.3 The Firewall Rule Screen

You may define firewall rules to allow or block certain types of traffic in or out of your network.

For example, you may create rules to:

- Block certain types of traffic, such as Telnet, from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow someone on the WAN to access a web server on your LAN.

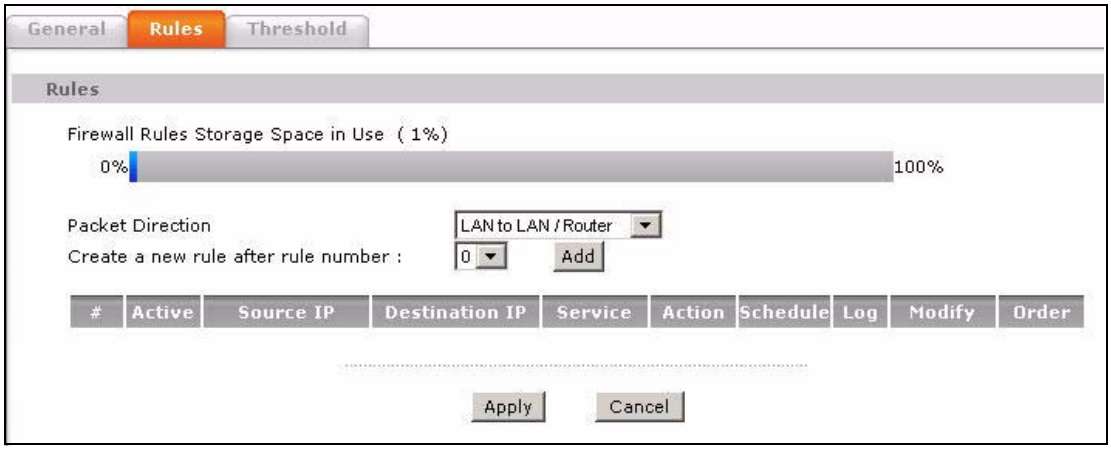
These custom rules work by comparing the source IP address, destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the ZyXEL Device's default rules.

Note: The ordering of your rules is very important as rules are applied in turn.

Refer to Section 9.5 on page 200 for more information.

Select **Custom** from the **General** screen. The **Rules** tab will appear. Click the tab to go to **Rules** screen. This screen displays a list of the configured firewall rules. Note the order in which the rules are listed.

Figure 62 Security > Firewall > Rules



The following table describes the labels in this screen.

Table 46 Security > Firewall > Rules

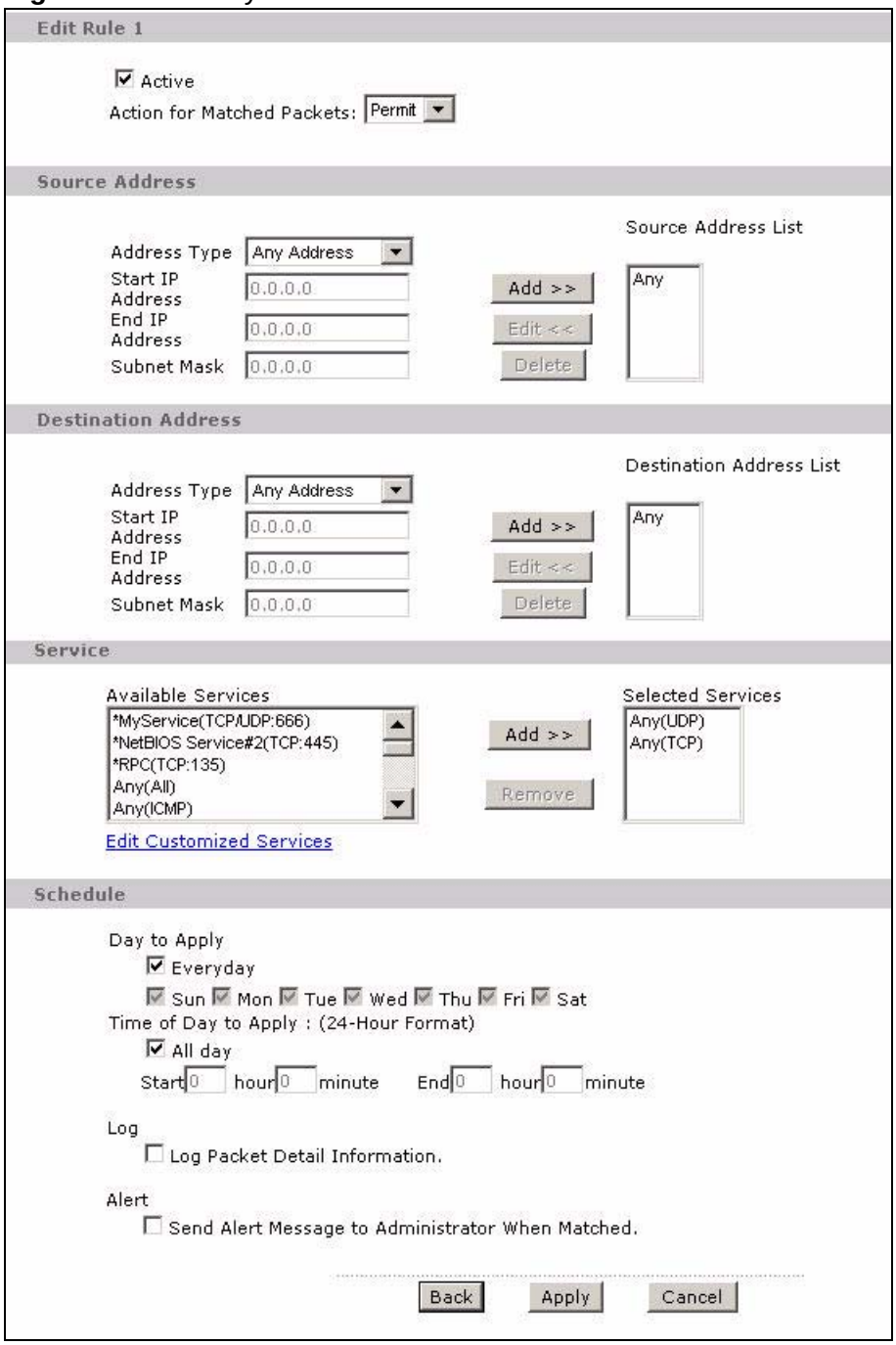
LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This read-only bar shows how much of the ZyXEL Device's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Create a new rule after rule number	Select an index number and click **Add** to add a new firewall rule after the selected index number. For example, if you select "1", your new rule becomes number 2 and the previous rule 2 (if there is one) becomes rule 3.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings in the **General** screen.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Active	This field displays whether a firewall is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule.
Source IP	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Destination IP	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Service	This drop-down list box displays the services to which this firewall rule applies. See Appendix E on page 421 for more information.
Action	This field displays whether the firewall silently discards packets (**Drop**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**Reject**) or allows the passage of packets (**Permit**).
Schedule	This field tells you whether a schedule is specified (**Yes**) or not (**No**).
Log	This field shows you whether a log is created when packets match this rule (**Yes**) or not (**No**).
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Order	Click the Move icon to display the **Move the rule to** field. Type a number in the **Move the rule to** field and click the **Move** button to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

9.3.1 Configuring Firewall Rules

Refer to Section 9.1.2 on page 182 for more information.

Use this screen to configure firewall rules. In the **Rules** screen, select an index number and click **Add** or click a rule's **Edit** icon to display this screen and refer to the following table for information on the labels.

Figure 63 Security > Firewall > Rules: Edit



The following table describes the labels in this screen.

Table 47 Security > Firewall > Rules: Edit

LABEL	DESCRIPTION
Edit Rule	
Active	Select this option to enable this firewall rule.
Action for Matched Packet	Use the drop-down list box to select whether to discard (**Drop**), deny and send an ICMP destination-unreachable message to the sender of (**Reject**) or allow the passage of (**Permit**) packets that match this rule.
Source/Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for instance, 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**.
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add >>	Click **Add >>** to add a new address to the **Source** or **Destination Address** box. You can add multiple addresses, ranges of addresses, and/or subnets.
Edit <<	To edit an existing source or destination address, select it from the box and click **Edit <<**.
Delete	Highlight an existing source or destination address from the **Source** or **Destination Address** box above and click **Delete** to remove it.
Services	
Available/ Selected Services	Please see Appendix E on page 421 for more information on services available. Highlight a service from the **Available Services** box on the left, then click **Add >>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **Remove**.
Edit Customized Service	Click the **Edit Customized Services** link to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select **All Day** or enter the start and end times in the hour-minute format to apply the rule.
Log	
Log Packet Detail Information	This field determines if a log for packets that match the rule is created or not. Go to the **Log Settings** page and select the **Access Control** logs category to have the ZyXEL Device record these logs.
Alert	

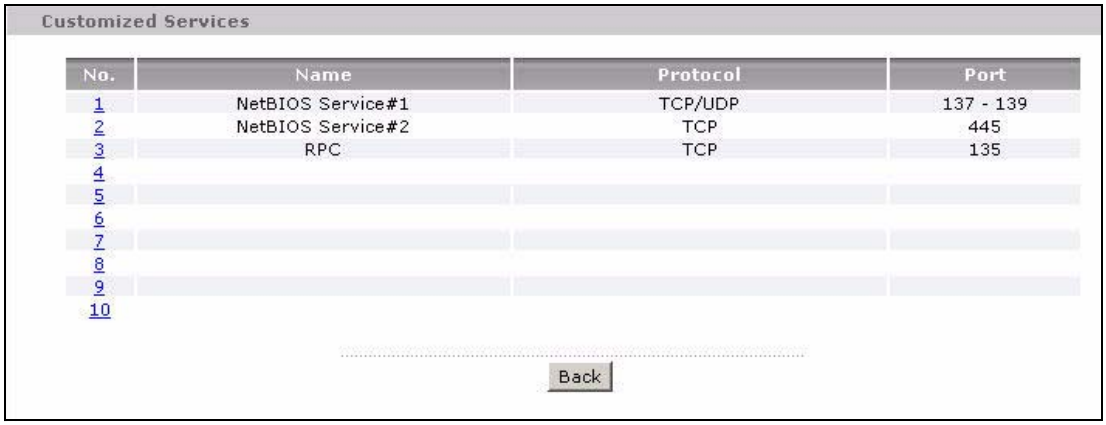
Table 47 Security > Firewall > Rules: Edit (continued)

LABEL	DESCRIPTION
Send Alert Message to Administrator When Matched	Select the check box to have the ZyXEL Device generate an alert when the rule is matched.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

9.3.2 Customized Services

Configure customized services and port numbers not predefined by the ZyXEL Device. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See Appendix E on page 421 for some examples. Click the **Edit Customized Services** link while editing a firewall rule to configure a custom service port. This displays the following screen.

Figure 64 Security > Firewall > Rules: Edit: Edit Customized Services



The following table describes the labels in this screen.

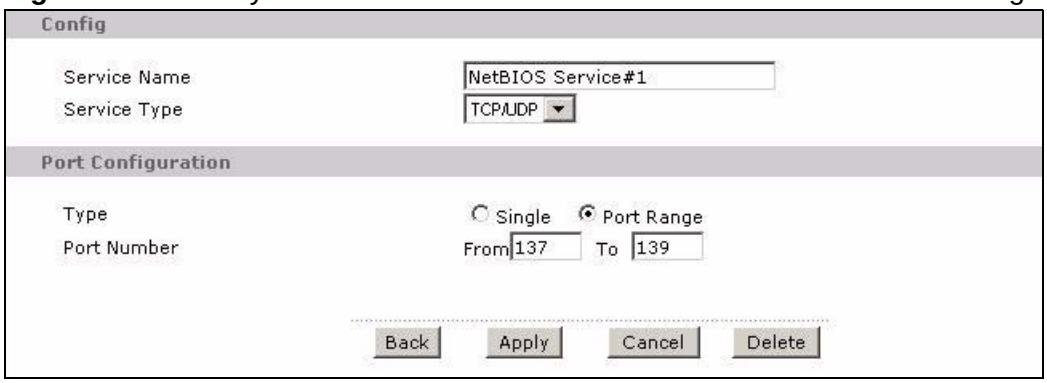
Table 48 Security > Firewall > Rules: Edit: Edit Customized Services

LABEL	DESCRIPTION
No.	This is the number of your customized port. Click a rule's number of a service to go to the **Firewall Customized Services Config** screen to configure or edit a customized service.
Name	This is the name of your customized service.
Protocol	This shows the IP protocol (**TCP**, **UDP** or **TCP/UDP**) that defines your customized service.
Port	This is the port number or range that defines your customized service.
Back	Click this to return to the **Firewall Edit Rule** screen.

9.3.3 Configuring a Customized Service

Use this screen to add a customized rule or edit an existing rule. Click a rule number in the **Firewall Customized Services** screen to display the following screen.

Figure 65 Security > Firewall > Rules: Edit: Edit Customized Services: Config



The following table describes the labels in this screen.

Table 49 Security > Firewall > Rules: Edit: Edit Customized Services: Config

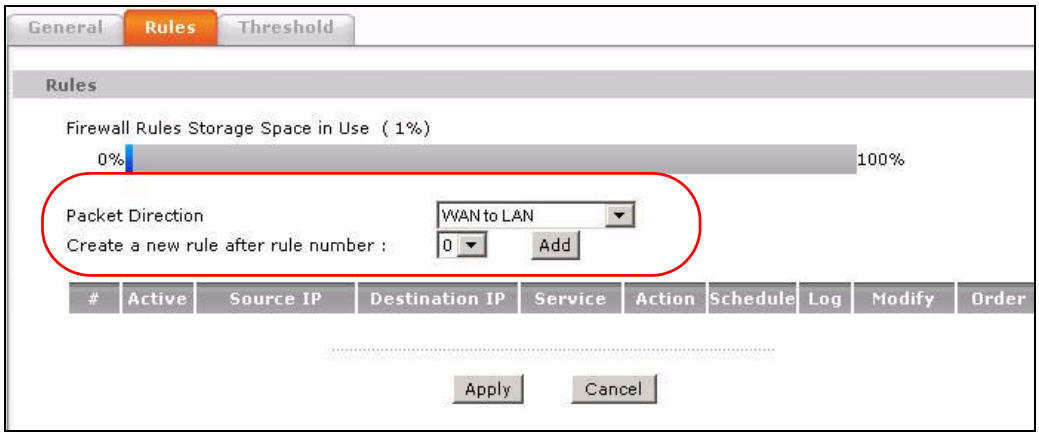
LABEL	DESCRIPTION
Config	
Service Name	Type a unique name for your custom port.
Service Type	Choose the IP port (**TCP**, **UDP** or **TCP/UDP**) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Delete	Click this to delete the current rule.

9.3.4 Firewall Rule Using a Customized Service Example

The following Internet firewall rule example allows a hypothetical “Doom” connection from the Internet.

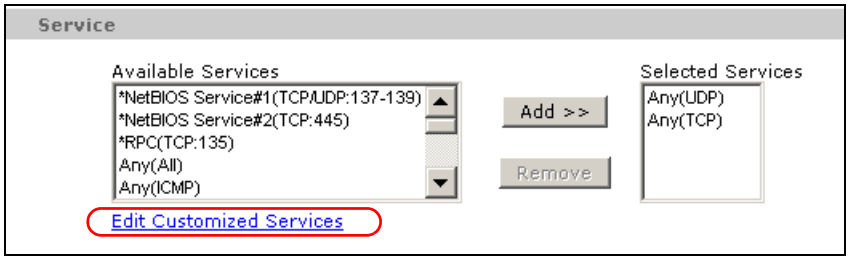
1 Select **Custom** from the **General** screen. The **Rules** tab will appear. Click the tab to go to **Rules** screen.

2 Select **WAN to LAN** in the **Packet Direction** field.

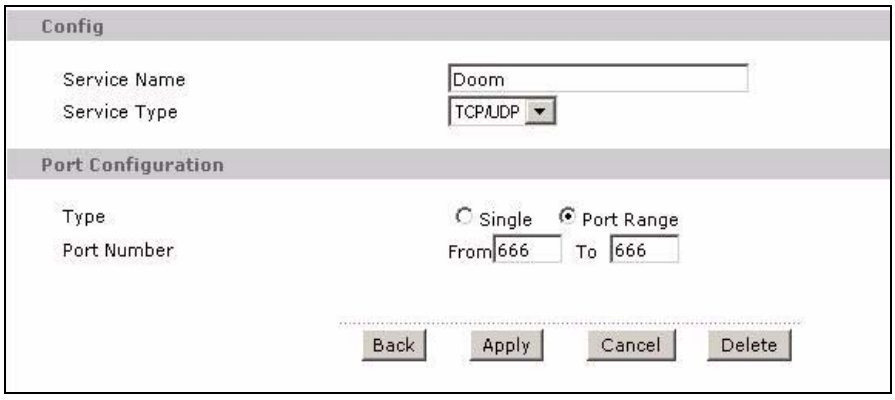


3 Click **Add** to display the firewall rule configuration screen.

4 In the **Edit Rule** screen, click the **Edit Customized Services** link to open the **Customized Service** screen.



5 Click an index number to display the **Customized Services Config** screen and configure the screen as follows and click **Apply**.

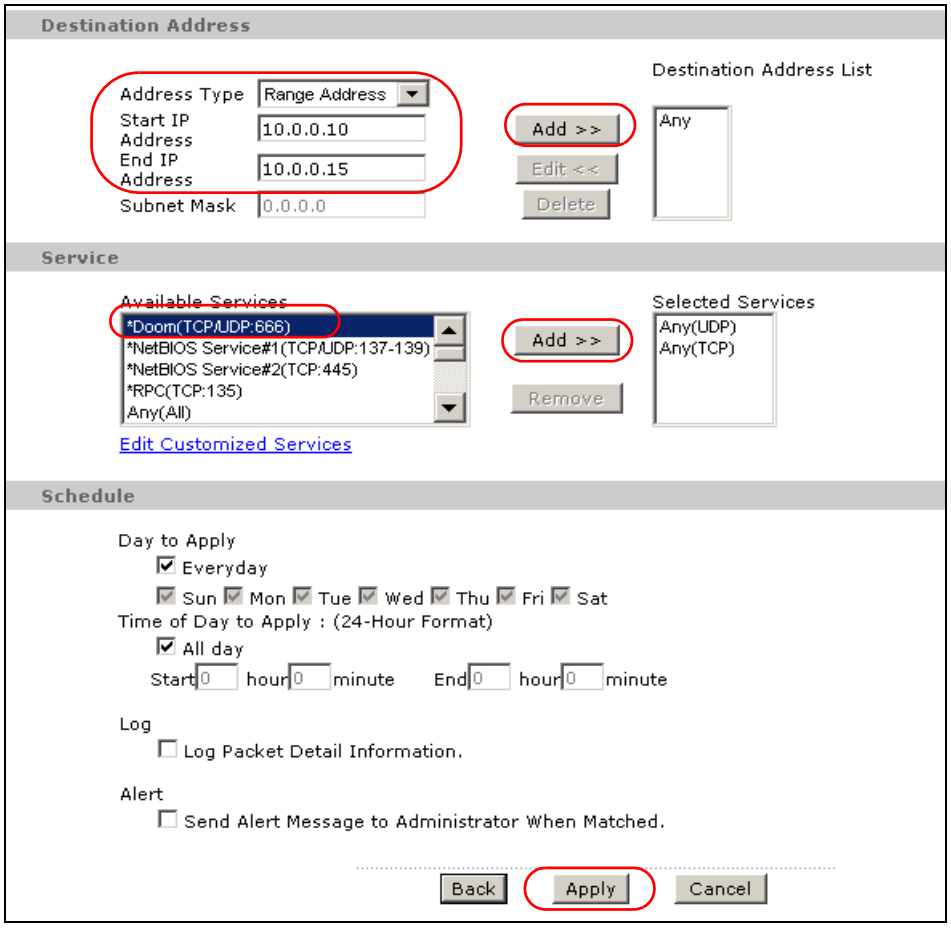


6 Return to the **Edit Rule** screen and configure the destination address screen and click **Add**. Delete **Any** from the Destination Address List.

7 Scroll down the Available Services list and select ***Doom(TCP/UDP:666)**. Use the **Add >>** button to add it to the Available Services list. Use the **Remove** button to remove services you do not need.

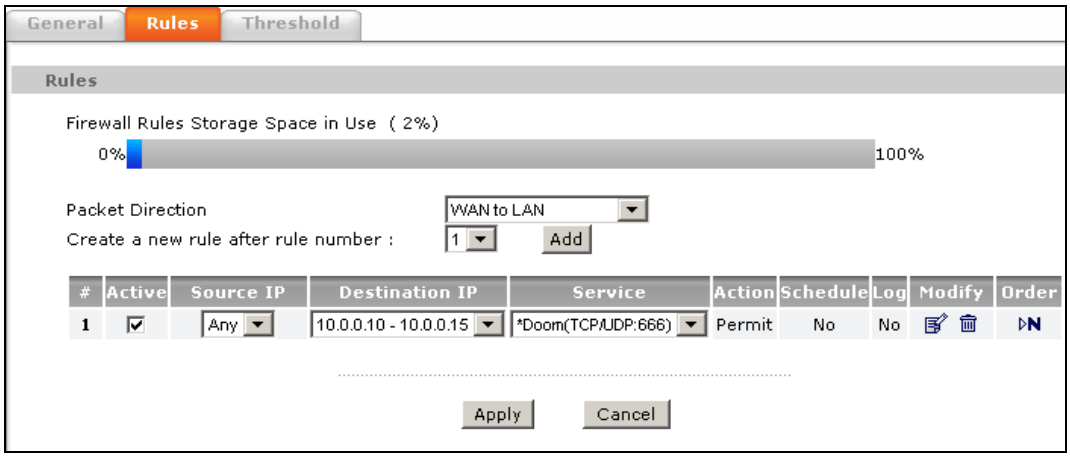
8 Configure other settings in **Schedule**. Click **Apply** when you are done.

Note: Custom services show up with an "*" before their names in the **Services** list box and the **Rules** list box.



On completing the configuration procedure for this Internet firewall rule, the **Rules** screen should look like the following.

Rule 1 allows a “MyService” connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

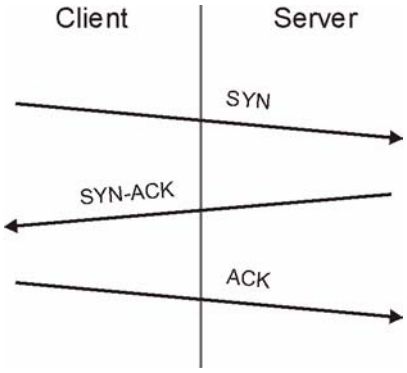


9.4 The Firewall Threshold Screen

For DoS attacks, the ZyXEL Device uses thresholds to determine when to start dropping sessions that do not become fully established (half-open sessions). These thresholds apply globally to all sessions.

For TCP, half-open means that the session has not reached the established state-the TCP three-way handshake has not yet been completed. Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

Figure 66 Three-Way Handshake



For UDP, half-open means that the firewall has detected no return traffic. An unusually high number (or arrival rate) of half-open sessions could indicate a DOS attack.

9.4.1 Threshold Values

If everything is working properly, you probably do not need to change the threshold settings as the default threshold values should work for most small offices. Tune these parameters when you believe the ZyXEL Device has been receiving DoS attacks that are not recorded in the logs or the logs show that the ZyXEL Device is classifying normal traffic as DoS attacks. Factors influencing choices for threshold values are:

1 The maximum number of opened sessions.

2 The minimum capacity of server backlog in your LAN network.

3 The CPU power of servers in your LAN network.

4 Network bandwidth.

5 Type of traffic for certain servers.

Reduce the threshold values if your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy).

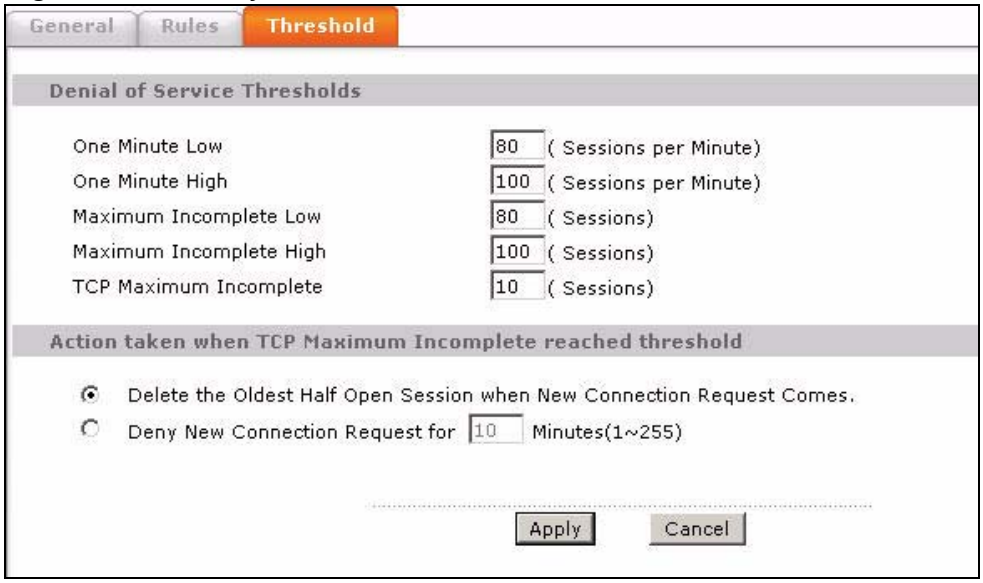
- If you often use P2P applications such as file sharing with eMule or eDonkey, it's recommended that you increase the threshold values since lots of sessions will be established during a small period of time and the ZyXEL Device may classify them as DoS attacks.

9.4.2 Configuring Firewall Thresholds

The ZyXEL Device also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections.

Click **Firewall** > **Threshold** to bring up the next screen.

Figure 67 Security > Firewall > Threshold



The following table describes the labels in this screen.

Table 50 Security > Firewall > Threshold

LABEL	DESCRIPTION
Denial of Service Thresholds	The ZyXEL Device measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.
One Minute Low	This is the rate of new half-open sessions per minute that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.
One Minute High	This is the rate of new half-open sessions per minute that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection attempts. For example, if you set the one minute high to 100, the ZyXEL Device starts deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute. It stops deleting half-open sessions when the number of session establishment attempts detected in a minute goes below the number set as the one minute low.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.

Table 50 Security > Firewall > Threshold (continued)

LABEL	DESCRIPTION
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number. For example, if you set the maximum incomplete high to 100, the ZyXEL Device starts deleting half-open sessions when the number of existing half-open sessions rises above 100. It stops deleting half-open sessions when the number of existing half-open sessions drops below the number set as the maximum incomplete low.
TCP Maximum Incomplete	An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host. Specify the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth. The ZyXEL Device sends alerts whenever the **TCP Maximum Incomplete** is exceeded.
Action taken when TCP Maximum Incomplete reached threshold	Select the action that ZyXEL Device should take when the TCP maximum incomplete threshold is reached. You can have the ZyXEL Device either: Delete the oldest half open session when a new connection request comes. or Deny new connection requests for the number of minutes that you specify (between 1 and 255).
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

9.5 Firewall Technical Reference

This section provides some technical background information about the topics covered in this chapter.

9.5.1 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.
2. Think about access control before you connect to the network in any way.

3 Limit who can access your router.

4 Don't enable any local service (such as telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.

5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.

6 Protect against IP spoofing by making sure the firewall is active.

7 Keep the firewall in a secured (locked) room.

9.5.2 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the ZyXEL Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?

2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

3 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.

4 Does this rule conflict with any existing rules?

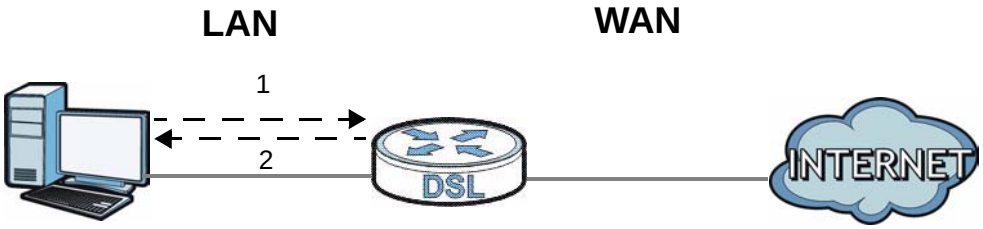
Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.

9.5.3 Triangle Route

When the firewall is on, your ZyXEL Device acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing

network traffic passes through the ZyXEL Device to protect your LAN against attacks.

Figure 68 Ideal Firewall Setup



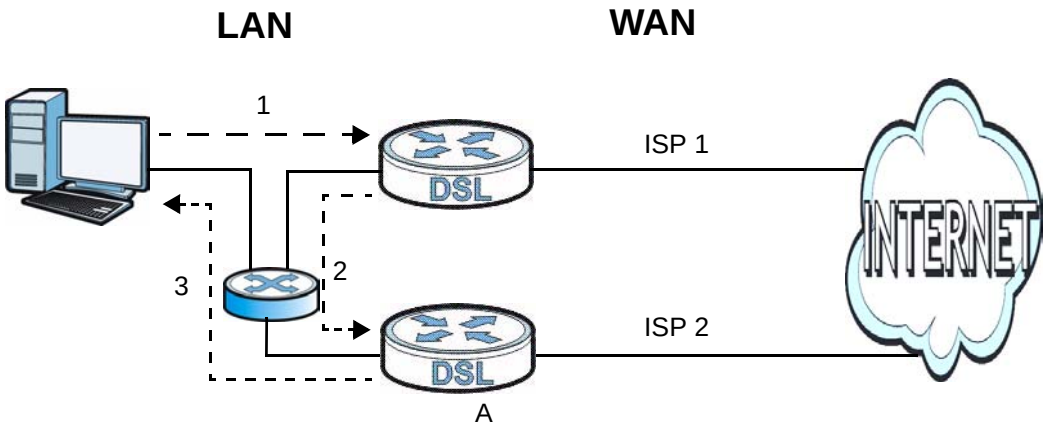
9.5.3.1 The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. You may have more than one connection to the Internet (through one or more ISPs). If an alternate gateway is on the LAN (and its IP address is in the same subnet as the ZyXEL Device’s LAN IP address), the “triangle route” (also called asymmetrical route) problem may occur. The steps below describe the “triangle route” problem.

1. A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
2. The ZyXEL Device reroutes the SYN packet through Gateway **A** on the LAN to the WAN.
3. The reply from the WAN goes directly to the computer on the LAN without going through the ZyXEL Device.

   As a result, the ZyXEL Device resets the connection, as the connection has not been acknowledged.

Figure 69 “Triangle Route” Problem



9.5.3.2 Solving the "Triangle Route" Problem

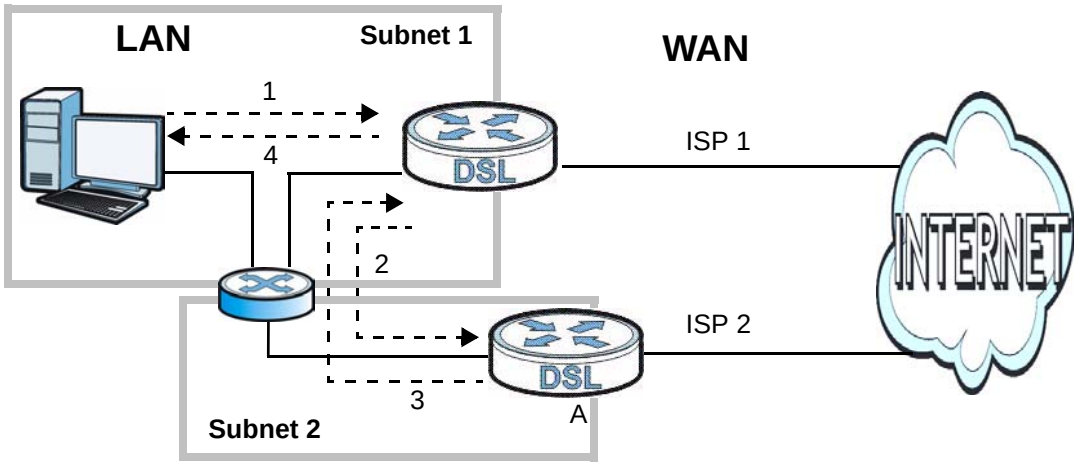
If you have the ZyXEL Device allow triangle route sessions, traffic from the WAN can go directly to a LAN computer without passing through the ZyXEL Device and its firewall protection.

Another solution is to use IP alias. IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your ZyXEL Device supports up to three logical LAN interfaces with the ZyXEL Device being the gateway for each logical network.

It's like having multiple LAN networks that actually use the same physical cables and ports. By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the ZyXEL Device to your LAN. The following steps describe such a scenario.

1. A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The ZyXEL Device reroutes the packet to Gateway A, which is in Subnet 2.
3. The reply from the WAN goes to the ZyXEL Device.
4. The ZyXEL Device then sends it to the computer on the LAN in Subnet 1.

Figure 70 IP Alias



10

Content Filtering

10.1 Overview

Internet content filtering allows you to block web sites based on keywords in the URL.

See Section 10.1.4 on page 206 for an example of setting up content filtering.

10.1.1 What You Can Do in the Content Filter Screens

- Use the **Keyword** screen (Section 10.2 on page 208) to block web sites based on a keyword in the URL.
- Use the **Schedule** screen (Section 10.3 on page 209) to specify the days and times keyword blocking is active.
- Use the **Trusted** screen (Section 10.4 on page 210) to exclude computers and other devices on your LAN from the keyword blocking filter.

10.1.2 What You Need to Know About Content Filtering

URL

The URL (Uniform Resource Locator) identifies and helps locate resources on a network. On the Internet the URL is the web address that you type in the address bar of your Internet browser, for example “http://www.zyxel.com”.

10.1.3 Before You Begin

To use the **Trusted** screen, you need the IP addresses of devices on your network. See the **LAN** section (Section 10.4 on page 210) for more information.

10.1.4 Content Filtering Example

The following shows the steps required for a parent (Bob) to set up content filtering on a home network in order to limit his children's access to certain web sites. In the following example, all URLs containing the word 'bad' are blocked.

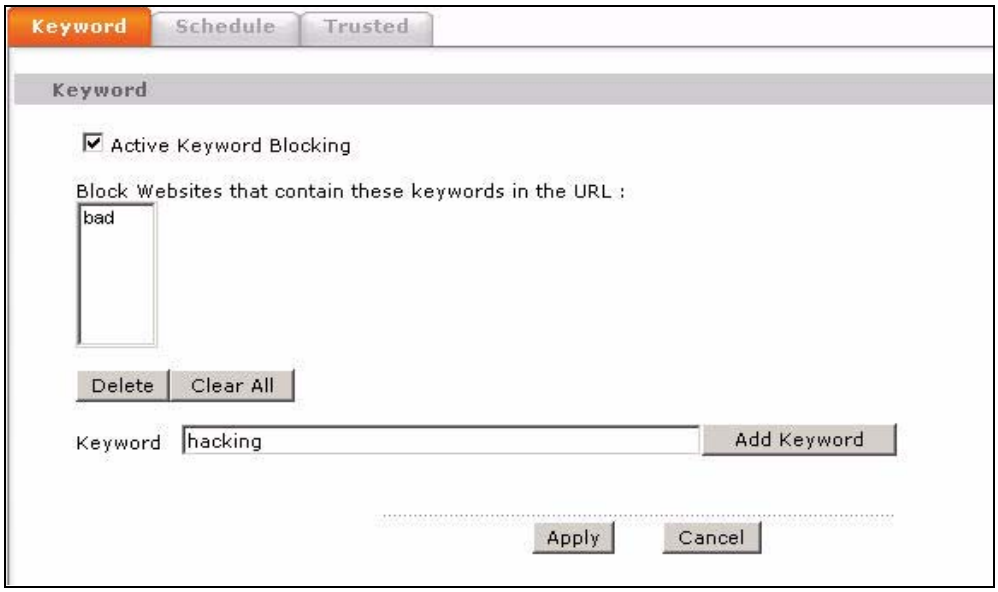
1 Click **Security > Content Filter** to display the following screen.

2 Select **Active Keyword Blocking**.

3 In the **Keyword** field type keywords to identify websites to be blocked.

4 Click **Add Keyword** for each keyword to be entered.

5 Click **Apply**.



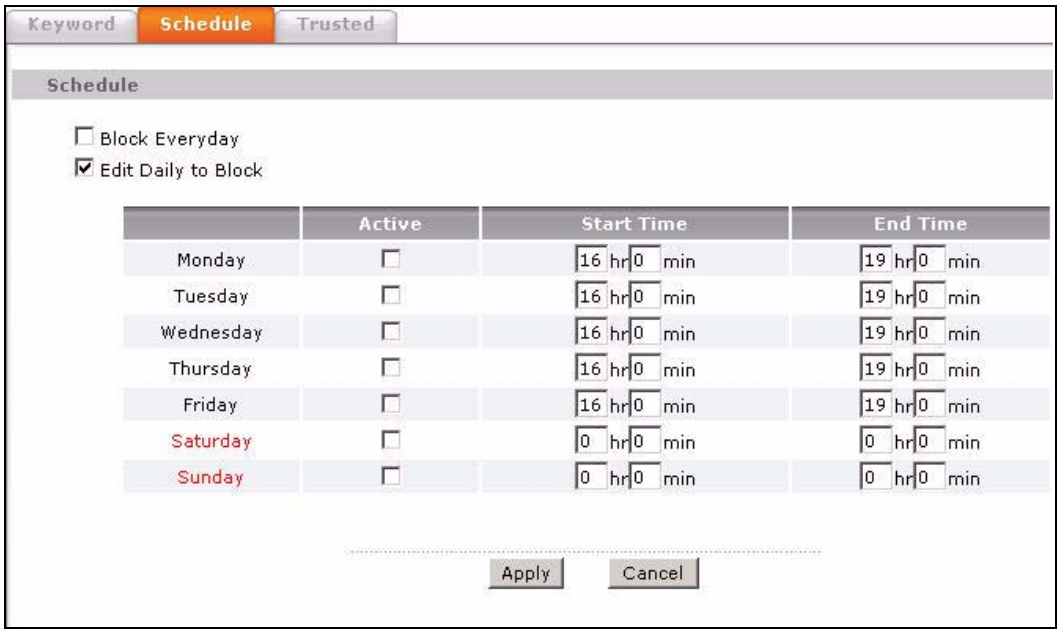
Bob's son arrives home from school at four, while his parents arrive later, at about 7pm. So keyword blocking is enabled for these times on weekdays and not on the weekend when the parents are at home.

1 Click **Security > Content Filter > Schedule**.

2 Click **Edit Daily to Block** and select all weekdays.

3 Under **Start Time** and **End Time**, type the times for blocking to begin and end (4pm ~ 7pm in this example).

4 Click **Apply**.



The children can access the family computer in the living room, while only the parents use another computer in the study room. So keyword blocking is only needed on the family computer and the study computer can be excluded from keyword blocking. Bob's home network is on the domain "192.168.1.xxx". Bob gave his home computer a static IP address of 192.168.1.2 and the study computer a static IP address of 192.168.1.3. To exclude the study computer from keyword blocking he follows these steps.

1 Click **Security > Content Filter** > **Trusted**.

2 In the **Start IP Address** and **End IP Address** fields, type 192.168.1.3.

3 Click **Apply**.

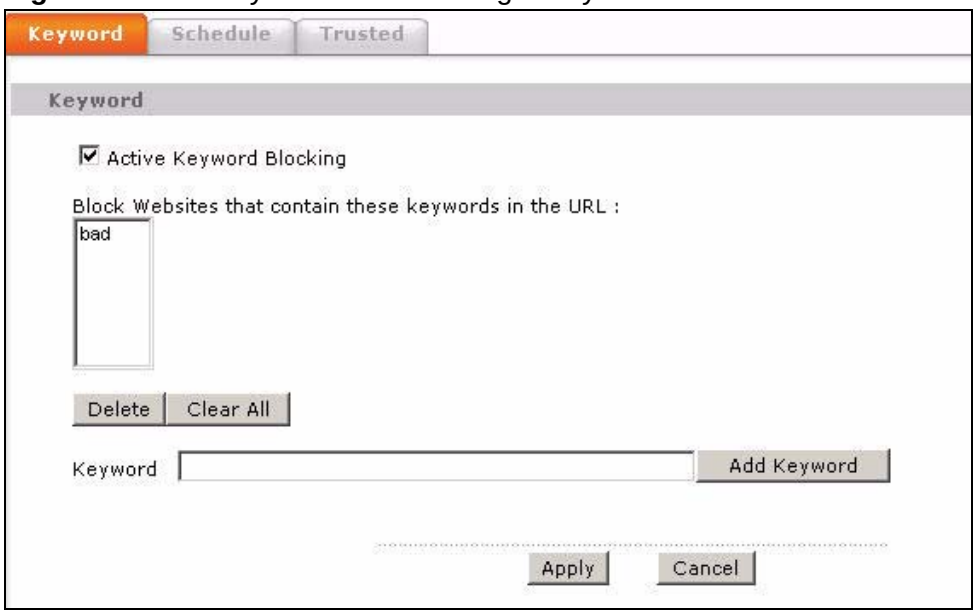
That finishes setting up keyword blocking on the home computer.

10.2 The Keyword Screen

Use this screen to block sites containing certain keywords in the URL. For example, if you enable the keyword "bad", the ZyXEL Device blocks all sites containing this keyword including the URL http://www.example.com/bad.html.

To have your ZyXEL Device block websites containing keywords in their URLs, click **Security > Content Filter**. The screen appears as shown.

Figure 71 Security > Content Filtering > Keyword



The following table describes the labels in this screen.

Table 51 Security > Content Filtering > Keyword

LABEL	DESCRIPTION
Active Keyword Blocking	Select this check box to enable this feature.
Block Websites that contain these keywords in the URL:	This box contains the list of all the keywords that you have configured the ZyXEL Device to block.
Delete	Highlight a keyword in the box and click this to remove it.
Clear All	Click this to remove all of the keywords from the list.
Keyword	Type a keyword in this field. You may use any character (up to 127 characters). Wildcards are not allowed.
Add Keyword	Click this after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.

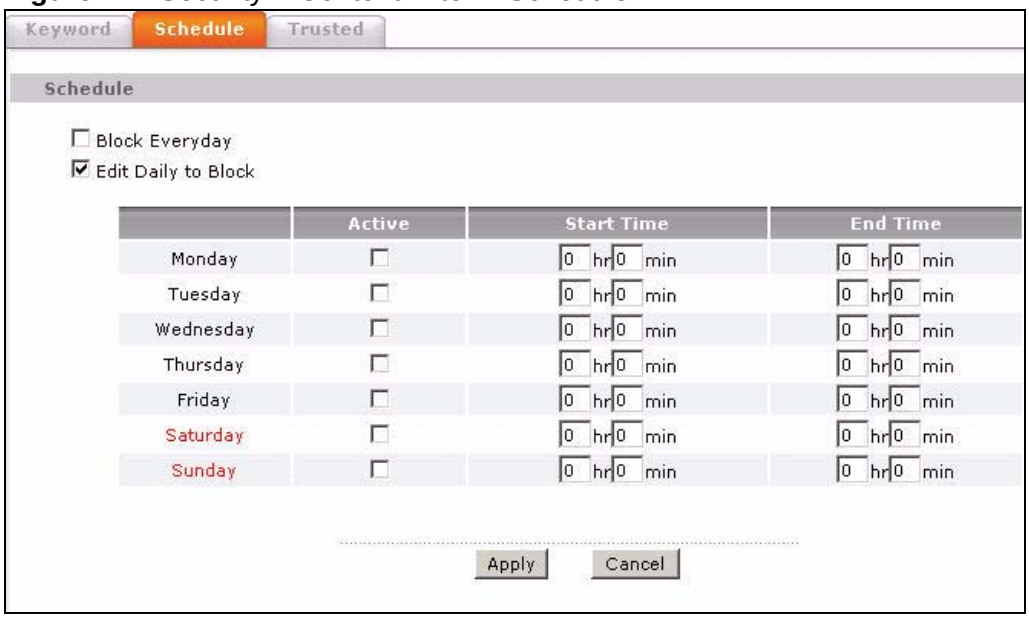
Table 51 Security > Content Filtering > Keyword (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

10.3 The Schedule Screen

Use this screen to set the days and times for the ZyXEL Device to perform content filtering. Click **Security > Content Filter** > **Schedule**. The screen appears as shown.

Figure 72 Security > Content Filter > Schedule



The following table describes the labels in this screen.

Table 52 Security > Content Filter: Schedule

LABEL	DESCRIPTION
Schedule	Select **Block Everyday** to make the content filtering active everyday. Otherwise, select **Edit Daily to Block** and configure which days of the week (or everyday) and which time of the day you want the content filtering to be active.
Active	Select the check box to have the content filtering to be active on the selected day.
Start TIme	Enter the time when you want the content filtering to take effect in hour-minute format.
End Time	Enter the time when you want the content filtering to stop in hour-minute format.

Table 52 Security > Content Filter: Schedule (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

10.4 The Trusted Screen

Use this screen to exclude a range of users on the LAN from content filtering on your ZyXEL Device. Click **Security > Content Filter** > **Trusted**. The screen appears as shown.

Figure 73 Security > Content Filter: Trusted

The following table describes the labels in this screen.

Table 53 Security > Content Filter: Trusted

LABEL	DESCRIPTION
Start IP Address	Type the IP address of a computer (or the beginning IP address of a specific range of computers) on the LAN that you want to exclude from content filtering.
End IP Address	Type the ending IP address of a specific range of users on your LAN that you want to exclude from content filtering. Leave this field blank if you want to exclude an individual computer.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

11

Packet Filter

11.1 Overview

Your ZyXEL Device uses filters to decide whether to allow passage of traffic. This chapter discusses how to create and apply filters.

11.1.1 What You Can Do in the Packet Filter Screen

Use the **Packet Filter** screens (Section 11.2 on page 212) to display the filter sets and configure the rules for protocol and generic filters.

11.1.2 What You Need to Know About the Packet Filter

Filters

Your ZyXEL Device uses filters to decide whether to allow passage of a data packet. Filters are subdivided into generic and protocol filters. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on IP packets.

Filter Structure

A filter set consists of one or more filter rules. The ZyXEL Device allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix generic filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

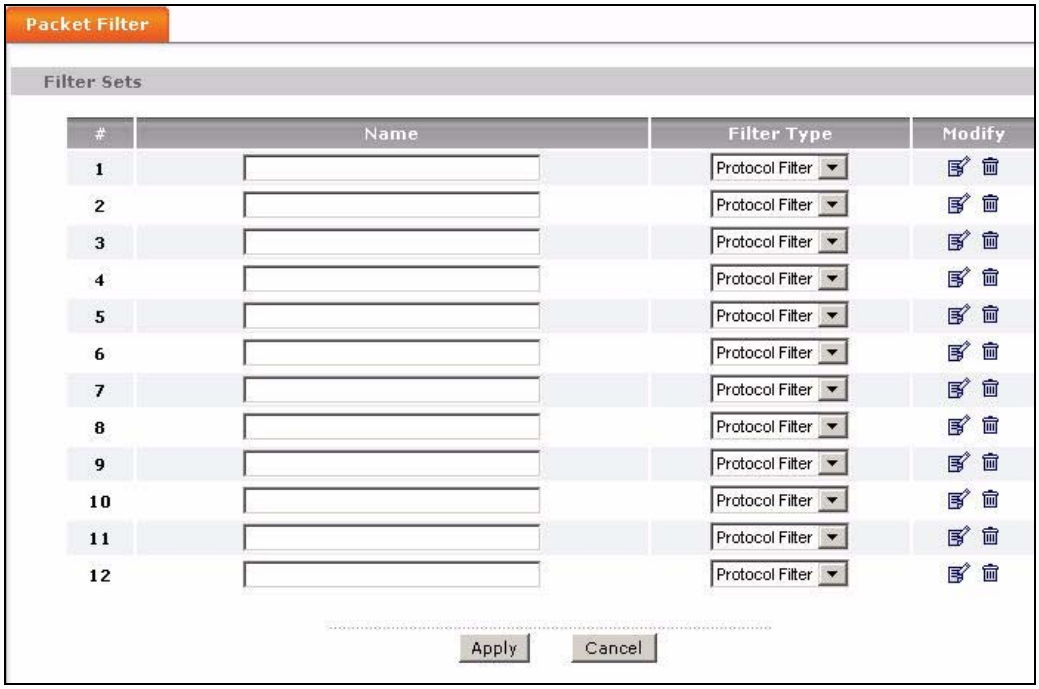
Finding Out More

See Section 11.3 on page 219 for technical background information on packet filters.

11.2 The Packet Filter Screen

Use this screen to set up packet filters on your ZyXEL Device. Click **Security > Packet Filter** to display the following screen.

Figure 74 Security > Packet Filter



The following table describes the labels in this screen.

Table 54 Security > Packet Filter

LABEL	DESCRIPTION
#	This field displays the index number of the filter set.
Name	Enter a name for the filter set. The text may consist of up to 16 letters, numerals and any printable character found on a typical English language keyboard.
Filter Type	Select **Protocol Filter** or **Generic Filter** for your filter set. Protocol filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.
Modify	Click the **Edit** button to configure a filter set. Click the **Remove** button to delete a filter set.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

11.2.1 Reset to Factory Defaults

There are two methods of resetting to factory defaults.

1 In the GUI go to **Maintenance** > **Update/Reboot** > **Configuration**. Click the **Reset** button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults.

2 If you forgot your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory default configuration file. This means that you will lose all configurations that you had previously and the password will reset to “broadband1”.

11.2.1.1 Using the RESET Button

1 Make sure that the **Power** LED is on (not blinking).

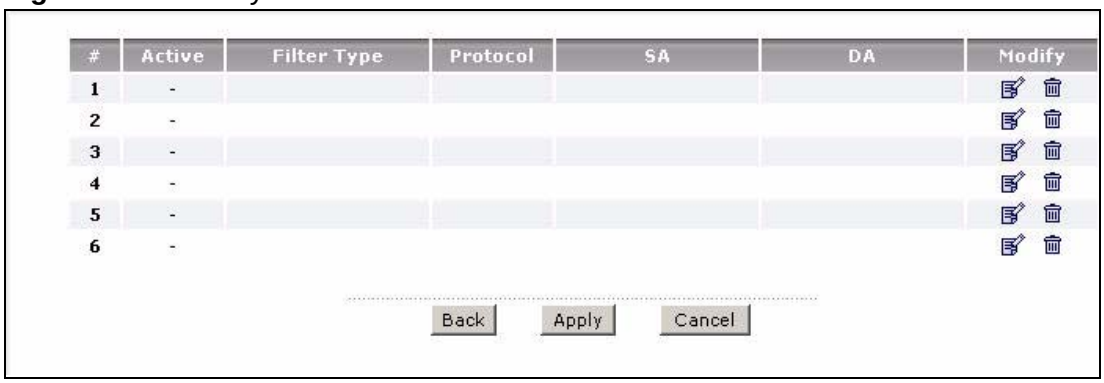
2 To set the device back to the factory default settings, press the **RESET** button for 5 seconds or until the **Power** LED begins to blink. Do not turn off the device while the reset is in progress! When the **Power** LED stops blinking and lights green, the defaults have been restored and the device restarts.

11.2.2 Editing Protocol Filters

Use this screen to display a protocol filter set on your ZyXEL Device. Protocol rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

In the **Packet Filter** screen, select **Protocol Filter** from the **Filter Type** field. Then click the **Edit** button from the **Modify** field to display the following screen.

Figure 75 Security > Packet Filter > Filter Rules



The following table describes the labels in this screen.

Table 55 Security > Packet Filter > Edit (Protocol Filter)

LABEL	DESCRIPTION
#	This is the index number of the rules in a filter set.
Active	Use the check box to turn a filter rule on or off.

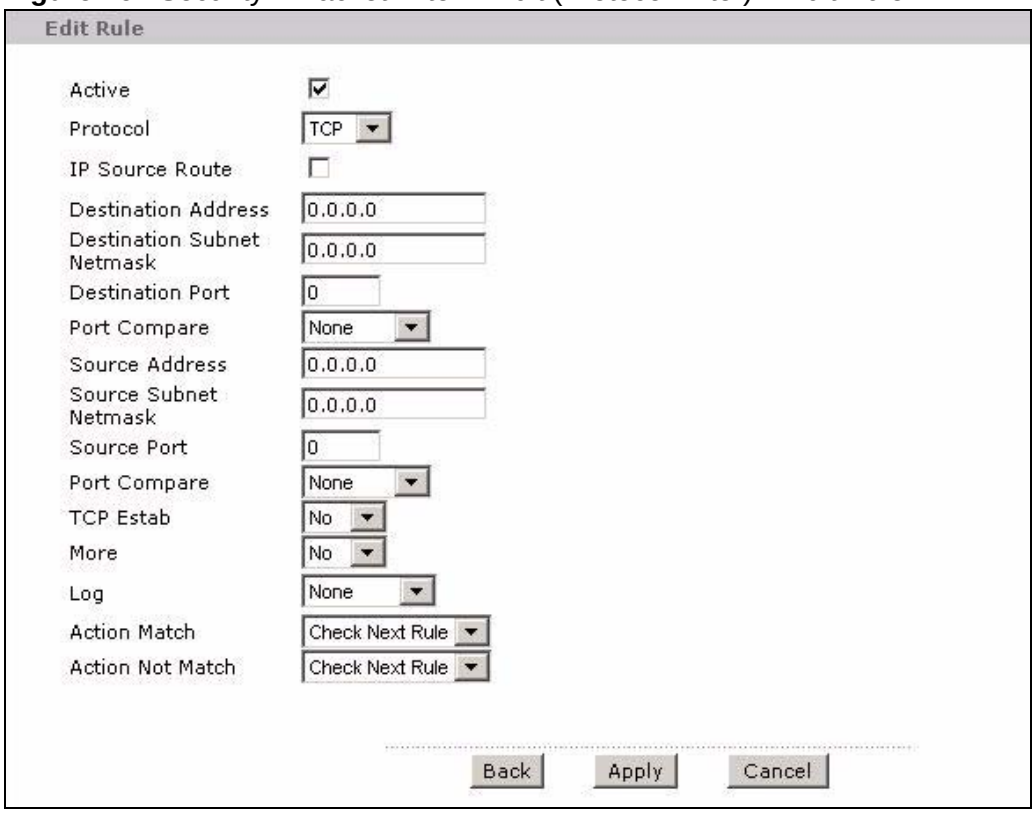
Table 55 Security > Packet Filter > Edit (Protocol Filter) (continued)

LABEL	DESCRIPTION
Filter Type	This field displays whether the filter type is a protocol filter or generic filter.
Protocol	This field displays the upper layer protocol.
SA	This field displays the source IP address.
DA	This field displays the destination IP address.
Modify	Click the **Edit** icon to configure a filter rule. Click the **Remove** icon to delete a filter rule.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

11.2.3 Configuring Protocol Filter Rules

Use this screen to configure protocol filter rules. In the **Edit (Protocol Filter)** screen, click an **Edit** icon to display the following screen.

Figure 76 Security > Packet Filter > Edit (Protocol Filter) > Edit Rule



The following table describes the labels in this screen.

Table 56 Security > Packet Filter > Edit (Protocol Filter) > Edit Rule

LABEL	DESCRIPTION
Active	Select the check box to enable the filter rule.
Protocol	Select **ICMP**, **TCP** or **UDP** for the upper layer protocol.
IP Source Route	Select the check box to apply the filter rule to packets with an IP source route option. The majority of IP packets do not have source route.
Destination Address	Enter the destination IP address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
Destination Subnet Netmask	Enter the IP subnet mask for the destination IP address.
Destination Port	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Port Compare	Select the comparison to apply to the destination port in the packet against the value given in the **Destination Port** field. Options are **None**, **Equal**, **Not Equal**, **Less** and **Greater**.
Source Address	Enter the source IP address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
Source Subnet Netmask	Enter the IP subnet mask for the source IP address
Source Port	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Port Compare	Select the comparison to apply to the source port in the packet against the value given in the **Source Port** field. Options are **None**, **Equal**, **Not Equal**, **Less** and **Greater**.
TCP Estab	This field is only available when you select **TCP** in the **Protocol** field. Select **Yes** to have the rule match packets that want to establish a TCP connection. This field is ignored if you select **No**.
More	Select **Yes** to pass a matching packet to the next filter rule before an action is taken. Select **No** to act upon the packet according to the action fields.
Log	Select a logging option from the following: **None** – No packets will be logged. **Match** - Only packets that match the rule parameters will be logged. **Not Match** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Match	Select the action for a matching packet. Options are **Check Next Rule**, **Forward** and **Drop**.
Action Not Match	Select the action for a packet not matching the rule. Options are **Check Next Rule**, **Forward** and **Drop**.

Table 56 Security > Packet Filter > Edit (Protocol Filter) > Edit Rule (continued)

LABEL	DESCRIPTION
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

If you applied the protocol filter rule, it will be displayed on the **Security > Packet Filter > Edit** screen. Click the Edit icon if you want to modify the rule.

After you have configured the packet filters for incoming and outgoing traffic, you can apply them to the WAN Internet access in the **Network > Internet (WAN) > Internet Access Setup: Advanced Setup** screen. See Section 5.2.1 on page 92 for more information.

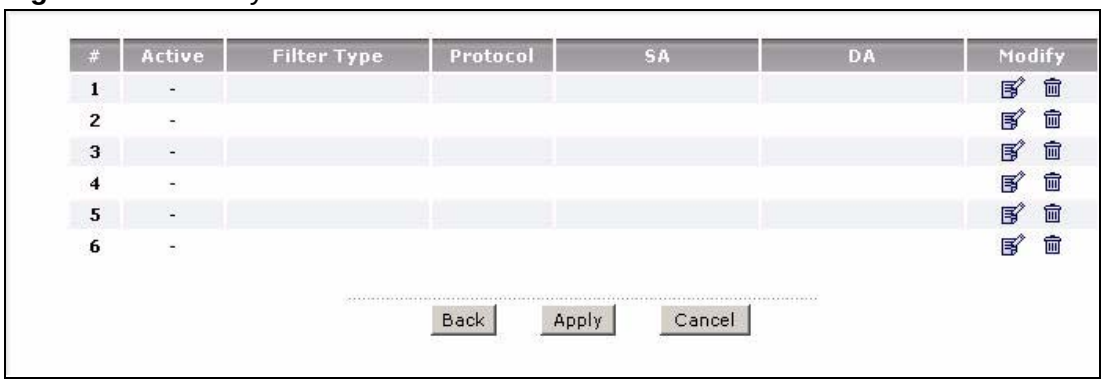
11.2.4 Editing Generic Filters

Use this screen to display a generic filter set on your ZyXEL Device. The purpose of generic rules is to allow you to filter non-IP packets. For IP packets, it is generally easier to use the IP rules directly.

For generic rules, the ZyXEL Device treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The ZyXEL Device applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4 bytes, the value in either field will take 8 digits, for example, FFFFFFFF.

In the **Packet Filter** screen, select **Generic Filter** from the **Filter Type** field. Then click the **Edit** button from the **Modify** field to display the following screen.

Figure 77 Security > Packet Filter > Filter Rules



The following table describes the labels in this screen.

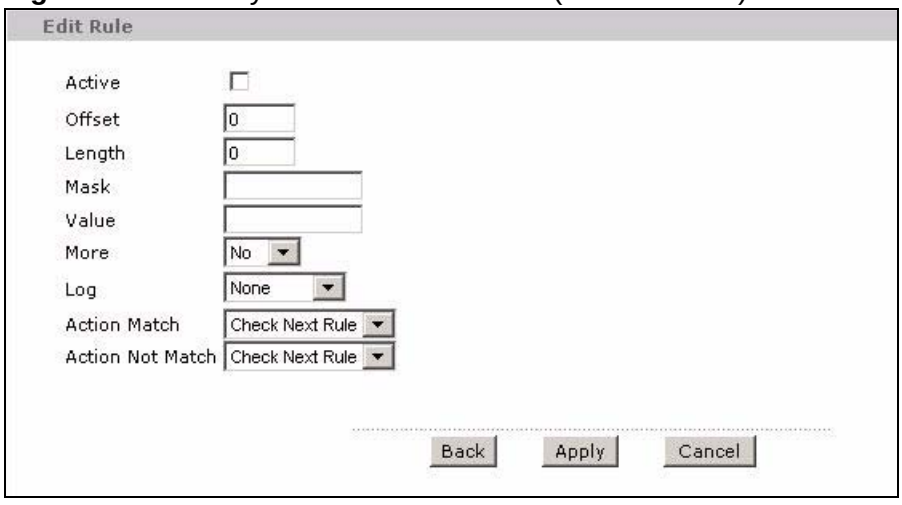
Table 57 Security > Packet Filter > Edit (Generic Filter)

LABEL	DESCRIPTION
#	This is the index number of the rules in a filter set.
Active	Use the check box to turn on or off a filter rule.
Filter Type	This field displays whether the filter type is a protocol filter or generic filter.
Offset	This field displays the offset value.
Length	This field displays the length value.
Mask	This field displays the mask value.
Value	This field displays the value.
Modify	Click the **Edit** icon to configure a filter rule. Click the **Remove** icon to delete a filter rule.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

11.2.5 Configuring Generic Packet Rules

Use this screen to configure generic filter rules. In the **Edit (Generic Filter)** screen, click the **Edit** button from the **Modify** field to display the following screen.

Figure 78 Security > Packet Filter > Edit (Generic Filter) > Edit Rule



The following table describes the labels in this screen.

Table 58 Security > Packet Filter > Edit (Generic Filter) > Edit Rule

LABEL	DESCRIPTION
Active	Select the check box to enable the filter rule.
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.
Mask	Enter the mask (in hexadecimal notation) to apply to the data portion before comparison.
Value	Enter the value (in hexadecimal notation) to compare with the data portion.
More	Select **Yes** to pass a matching packet to the next filter rule before an action is taken. Select **No** to act upon the packet according to the action fields.
Log	Select a logging option from the following: **None** – No packets will be logged. **Match** - Only packets that match the rule parameters will be logged. **Not Match** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Match	Select the action for a matching packet. Options are **Check Next Rule**, **Forward** and **Drop**.
Action Not Match	Select the action for a packet not matching the rule. Options are **Check Next Rule**, **Forward** and **Drop**.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

If you applied the generic filter rule, it will be displayed on the **Security > Packet Filter > Edit** screen. Click the Edit icon if you want to modify the rule.

After you have configured the packet filters for incoming and outgoing traffic, you can apply them to the WAN Internet access in the **Network > Internet (WAN) > Internet Access Setup: Advanced Setup** screen. See Section 5.2.1 on page 92 for more information.

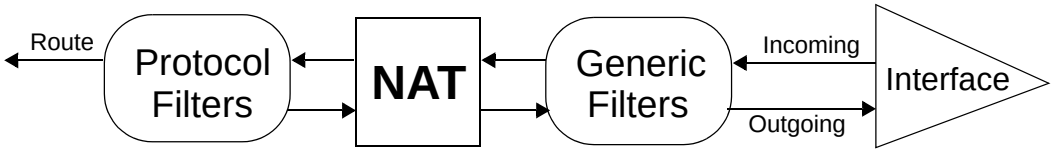
11.3 Packet Filter Technical Reference

This section provides some technical background information about the topics covered in this chapter.

11.3.1 Filter Types and NAT

There are two classes of filter rules, generic filter rules and protocol filter rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyXEL Device applies the protocol filters to the “native” IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic filters are applied to the raw packets that appear on the wire. They are applied at the point when the ZyXEL Device is receiving and sending the packets; that is the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

Figure 79 Protocol and Generic Filter Sets



11.3.2 Firewall Versus Filters

Below are some comparisons between the ZyXEL Device’s filtering and firewall functions.

Packet Filtering

- The router filters packets as they pass through the router’s interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

When To Use Filtering

- To block/allow LAN packets by their MAC addresses.
- To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.

- To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Generic filters cannot distinguish traffic originating from an inside host or an outside host by IP address or subnets.
- To block/allow IP trace route.

Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a non-existent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

When To Use The Firewall

- To prevent DoS attacks and prevent hackers cracking your network.
- A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.
- To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
- The firewall performs better than filtering if you need to check many rules.
- Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
- The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

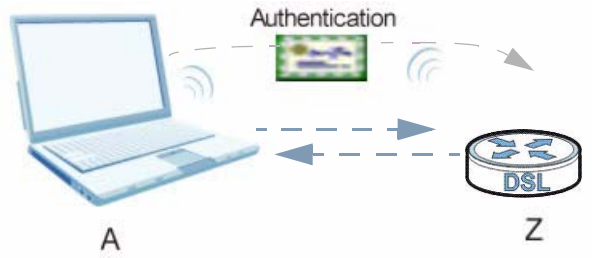
12 Certificates

12.1 Overview

This chapter describes how your ZyXEL Device can use certificates as a means of authenticating wireless clients. It gives background information about public-key certificates and explains how to use them.

A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Figure 80 Certificates Example



In the figure above, the ZyXEL Device (Z) checks the identity of the notebook (A) using a certificate before granting it access to the network.

12.1.1 What You Can Do in the Certificates Screens

Use the **Trusted CAs** screens (Section 12.2 on page 224) to save CA certificates to the ZyXEL Device.

12.1.2 What You Need to Know About Certificates

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyXEL Device to generate certification requests that contain identifying

information and public keys and then send the certification requests to a certification authority.

Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.

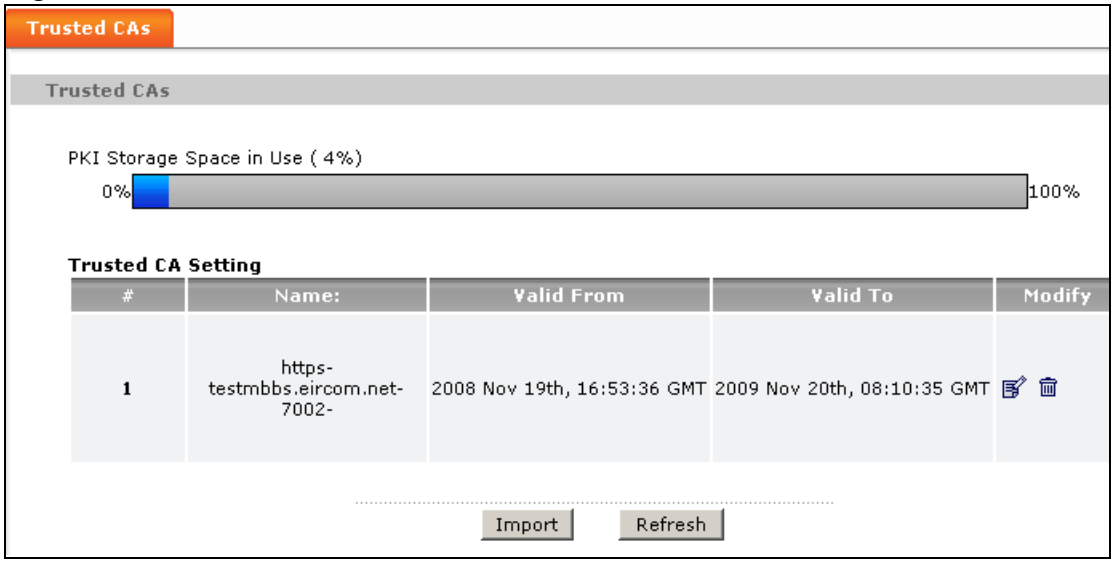
Finding Out More

See Section 12.3 on page 229 for technical background information on certificates.

12.2 The Trusted CAs Screen

This screen displays a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities. Click **Security > Certificates** to open the **Trusted CAs** screen.

Figure 81 Trusted CAs



The following table describes the labels in this screen.

Table 59 Trusted CAs

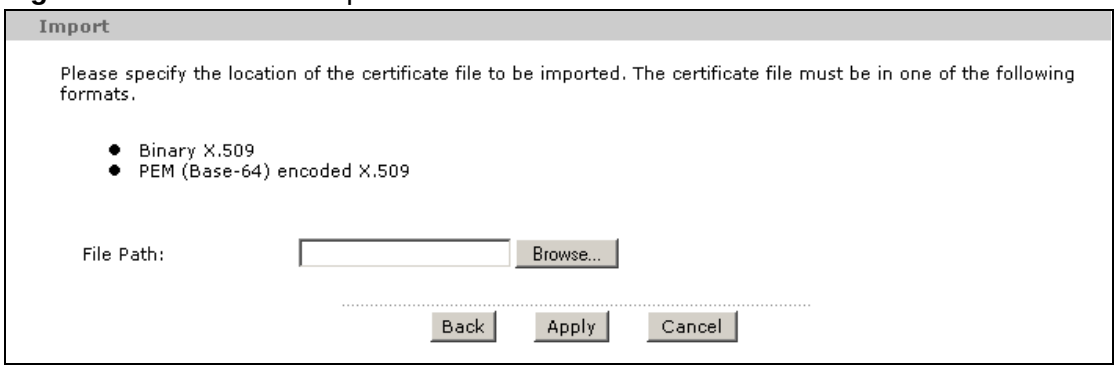
LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from blue to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the Edit icon to open a screen with an in-depth list of information about the certificate. Click the Remove icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action.
Import	Click this to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyXEL Device.
Refresh	Click this to display the current validity status of the certificates.

12.2.1 Trusted CA Import

Follow the instructions in this screen to save a trusted certification authority's certificate to the ZyXEL Device. Click **Security** > **Certificates** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 82 Trusted CA Import



The following table describes the labels in this screen.

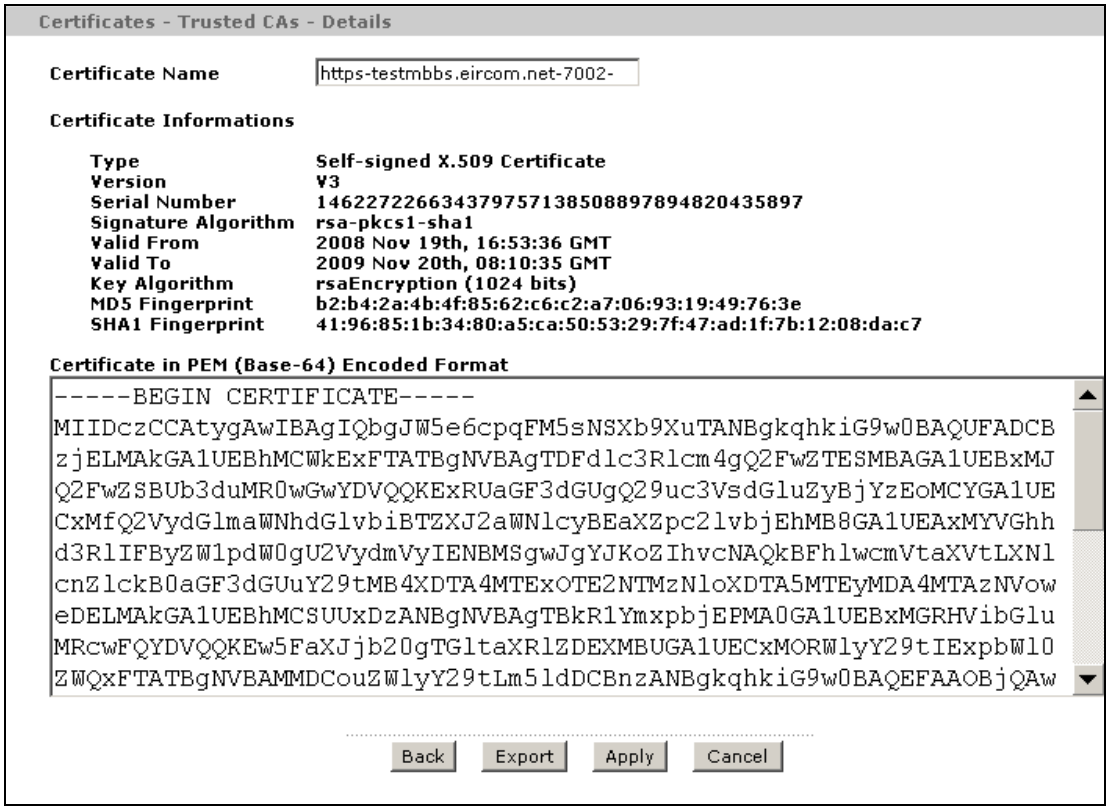
Table 60 Trusted CA Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click this to find the certificate file you want to upload.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save the certificate on the ZyXEL Device.
Cancel	Click this to restore your previously saved settings.

12.2.2 Trusted CA Details

Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority. Click **Security** > **Certificates** > **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen.

Figure 83 Trusted CA Details



The following table describes the labels in this screen.

Table 61 Trusted CA Details

LABEL	DESCRIPTION
Certificate Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.

Table 61 Trusted CA Details (continued)

LABEL	DESCRIPTION
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click this to return to the previous screen without saving.
Export	Click this and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Apply	Click this to save your changes. You can only change the name and/or set whether or not you want the ZyXEL Device to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click this to restore your previously saved settings.

12.3 Certificates Technical Reference

This section provides technical background information about the topics covered in this chapter.

12.3.1 Certificates Overview

The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

The ZyXEL Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

Advantages of Certificates

Certificates offer the following benefits.

- The ZyXEL Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

12.3.2 Private-Public Certificates

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

1. Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).

2. Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.

3. Tim uses his private key to sign the message and sends it to Jenny.

4. Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).

5. Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

PART IV
Advanced

WAN IP Passthrough (233)

Static Route (239)

VLANs (243)

Quality of Service (QoS) (253)

Dynamic DNS Setup (275)

Remote Management (279)

Universal Plug-and-Play (UPnP) (289)

13

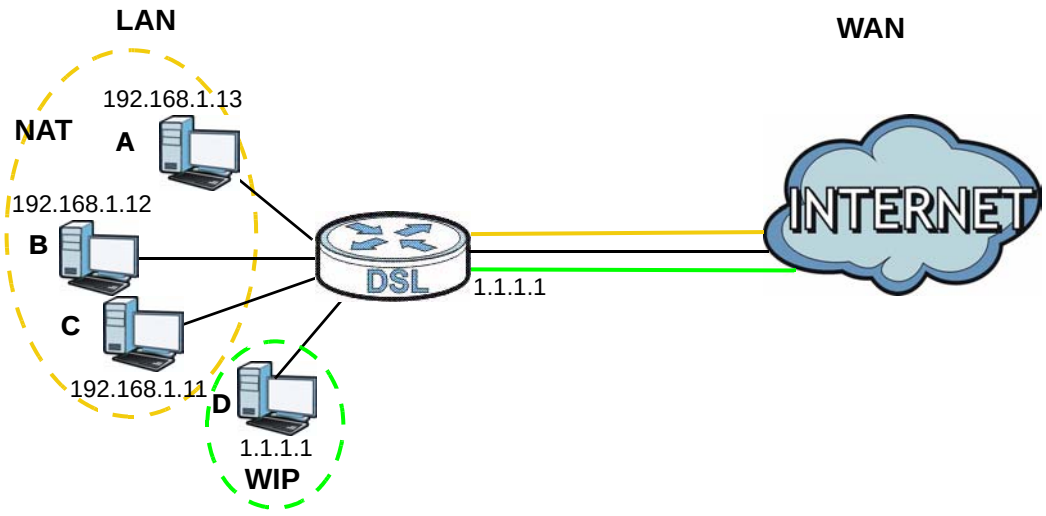
WAN IP Passthrough

13.1 The WAN IP Passthrough Screen

WAN IP Passthrough (WIP) allows a WAN computer on the local network of the ZyXEL Device to have access to web services using the public IP address. When WAN IP Passthrough is configured, all traffic is forwarded to the computer and will not go through NAT.

The following figure shows computers connected to the ZyXEL Device. Computers **A**, **B**, and **C** are connected to the ZyXEL Device's LAN interface with NAT enabled. They make up a private LAN and are assigned private IP addresses by the ZyXEL Device. Traffic to computer **D** does not go through NAT as it uses WAN IP Passthrough.

Example of WAN IP Passthrough Topology



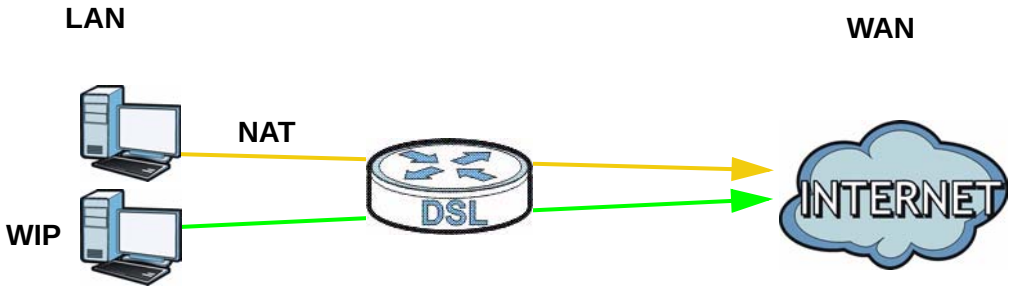
Use this feature on a LAN computer which runs applications that do not work well with NAT. For example, VOIP softphones using the SIP protocol may not work on a computer behind NAT.

13.1.1 What You Need to Know About IP Passthrough

Outgoing Traffic

Outgoing traffic from the WAN IP Passthrough computer to the WAN does not go through NAT.

Figure 84 Outgoing Traffic for WAN IP Passthrough

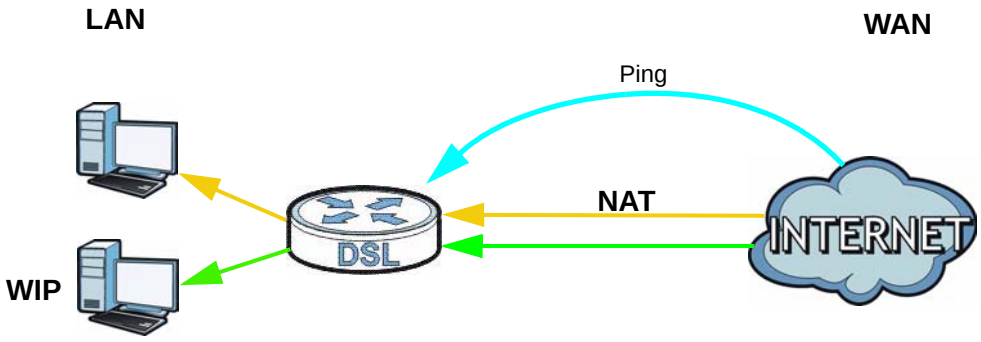


Incoming Traffic

If no NAT rule is found, then all traffic is forwarded to the WAN IP Passthrough computer except incoming ping traffic that goes to the ZyXEL Device.

Note: The default NAT server does not work when WAN IP Passthrough is enabled.

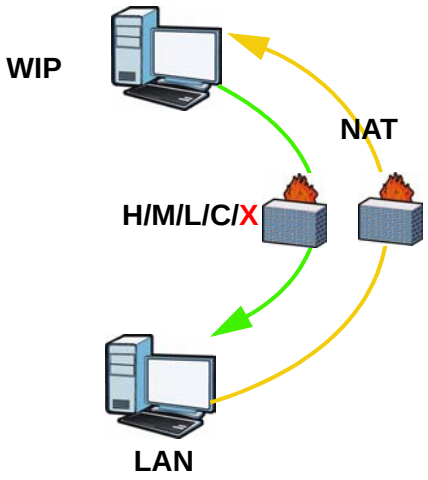
Figure 85 Incoming Traffic for WAN IP Passthrough



Intra-LAN Traffic

The WAN IP Passthrough computer can access a LAN computer with all firewall settings. But traffic from a LAN computer to the WAN IP Passthrough goes through the firewall and NAT.

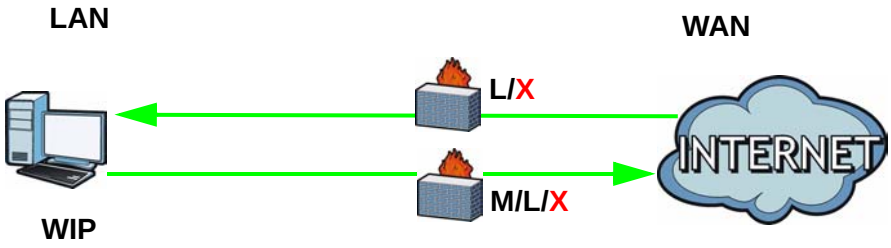
Figure 86 Intra-LAN Traffic



WAN IP Passthrough and the Firewall

If you want the WAN IP Passthrough computer to access the Internet, you must configure the firewall as **Medium**, **Low**, or **Off**. If you want to enable incoming traffic to the WAN IP Passthrough, you must configure the firewall as **Low** or **Off**. See Section 9.2 on page 186 for more information on configuring the firewall.

Figure 87 WAN IP Passthrough and the firewall



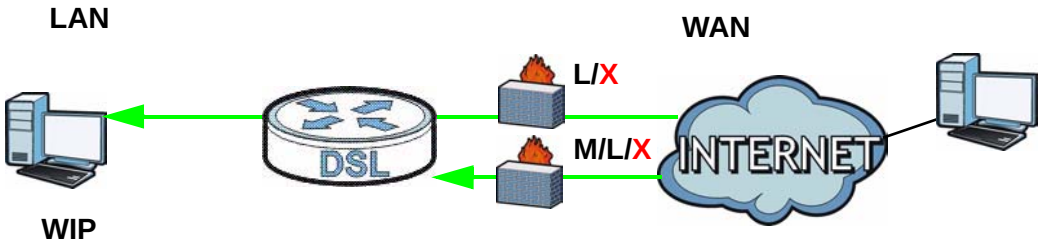
The table below shows the equivalent firewall rules when a LAN computer becomes a WAN IP Passthrough computer. For example, WIP to WAN traffic uses the LAN to WAN firewall rule. See Section 9.2.1 on page 186 for more information on firewall rules.

Table 62 Traffic Direction and Applicable

TRAFFIC DIRECTION	FIREWALL RULE
WIP to WAN	LAN to WAN
WAN to WIP	WAN to WAN/Router
WIP to LAN	LAN to LAN/Router
LAN to WIP	LAN to LAN/Router

WAN IP Passthrough and Remote Management

Figure 88 WAN IP Passthrough and Remote Management



If you configure the firewall as **Low** or **Off** and Remote Management is either activated or disabled, trusted computers from the WAN side can access the WAN IP Passthrough computer. If firewall is **Off** and Remote Management is activated, trusted computers from the WAN side can access the ZyXEL Device. If you configure the firewall as **Medium** or **High** and activate remote management, trusted computers from the WAN side can only have access to the ZyXEL Device. See Chapter 18 on page 279 for more information on Remote Management.

The table below explains the WAN access to WAN IP Passthrough computer and the ZyXEL Device with different firewall and Remote Management settings.

Table 63 WAN Access, Remote Management, and Firewall

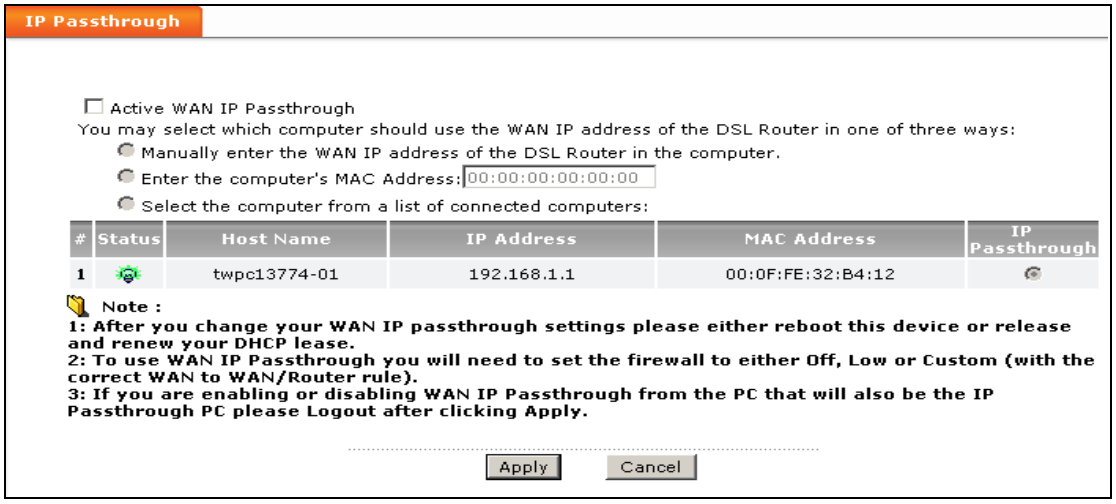
FIREWALL	REMOTE MANAGEMENT	ACCESS TO THE ZYXEL DEVICE	ACCESS TO THE WIP COMPUTER
Low/Off	Off	No	Yes
Off	On	Yes	No
Low	On	No	Yes
Medium/High	On	Yes	No

Use this screen to select the computer to use for WAN IP Passthrough. The selected computer cannot have a static IP address configured in **Network > Local Network (LAN) > Client List**.

Note: To use WAN IP Passthrough you will need to set the firewall to either **Off**, **Low** or **Custom** (with the correct WAN to WAN/Router rule).

Click **Advanced > WAN IP Passthrough** to open the **WAN IP Passthrough** screen.

Figure 89 Advanced > WAN IP Passthrough


IP Passthrough
Active WAN IP Passthrough
You may select which computer should use the WAN IP address of the DSL Router in one of three ways:
Manually enter the WAN IP address of the DSL Router in the computer.
Enter the computer's MAC Address: 00:00:00:00:00:00
Select the computer from a list of connected computers:
Status Host Name IP Address MAC Address IP Passthrough
1 twpc13774-01 192.168.1.1 00:0F:FE:32:B4:12
Note :
1: After you change your WAN IP passthrough settings please either reboot this device or release and renew your DHCP lease.
2: To use WAN IP Passthrough you will need to set the firewall to either Off, Low or Custom (with the correct WAN to WAN/Router rule).
3: If you are enabling or disabling WAN IP Passthrough from the PC that will also be the IP Passthrough PC please Logout after clicking Apply.
Apply
Cancel

The following table describes the labels in this screen.

Table 64 Advanced > IP Passthrough

LABEL	DESCRIPTION
Active WAN IP Passthrough	Select this to enable WAN IP Passthrough. After selecting it, choose which local computer will use the same WAN side IP address (public IP address) as the ZyXEL Device. Note: A WAN IP Passthrough computer cannot have a reserved static IP address in Network > Local Network(LAN) > Client List. Note: WAN IP Passthrough cannot work in Ethernet WAN mode. Clear this to disable the function.
Manually enter the WAN IP address of the DSL Router in the computer	Select this to manually enter the WAN IP address of the ZyXEL Device in the computer. You can find the IP address on the ZyXEL Device's Web Configurator **Status** page.
Enter the computer's MAC Address	Select this and enter the MAC address of the computer you want to configure IP Passthrough. Enter six pairs of hexadecimal notation with colons. See Section 6.4 on page 118 for more information on finding out your computer's MAC address.
Select the computer from a list of connected computers	Select this to choose a computer from the list of computers that the ZyXEL Device has assigned the addresses to.

Table 64 Advanced > IP Passthrough

LABEL	DESCRIPTION
#	This is the index number of the static IP table entry (row).
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the current computer name.
IP Address	This field displays the IP address of this computer.
MAC Address	Select this field to enter the MAC address of your computer.
IP Passthrough	Select the computer you want to configure with WAN IP Passthrough.
Apply	Click this to save your changes. After you click **Apply**, you need to renew the WAN IP Passthrough computer IP address.
Cancel	Click this to restore your previously saved settings.

14

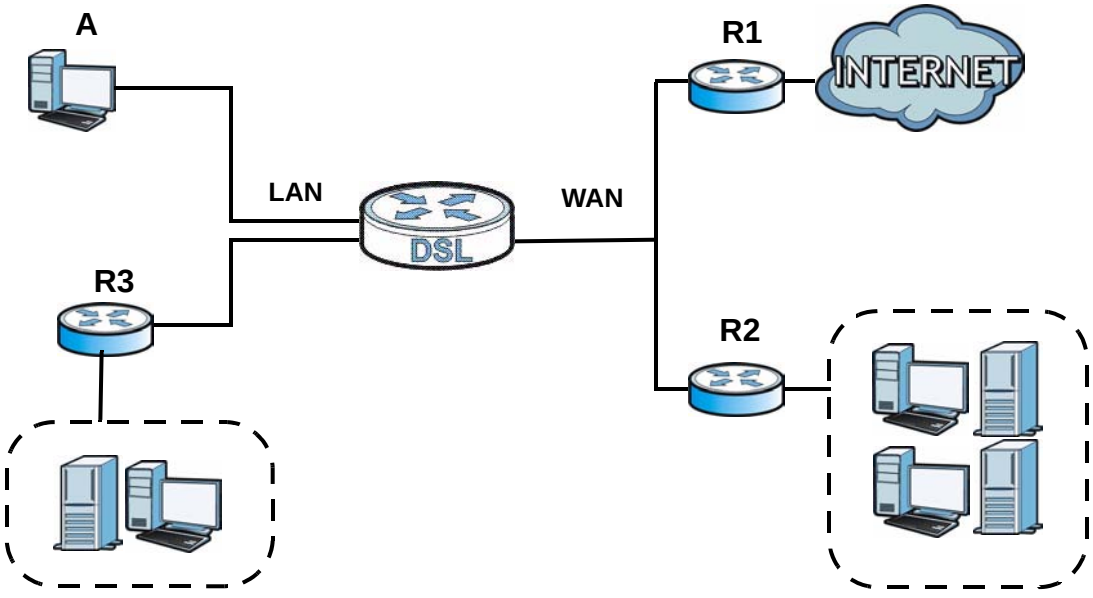
Static Route

14.1 Overview

The ZyXEL Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the ZyXEL Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the ZyXEL Device's LAN interface. The ZyXEL Device routes most traffic from **A** to the Internet through the ZyXEL Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 90 Example of Static Routing Topology



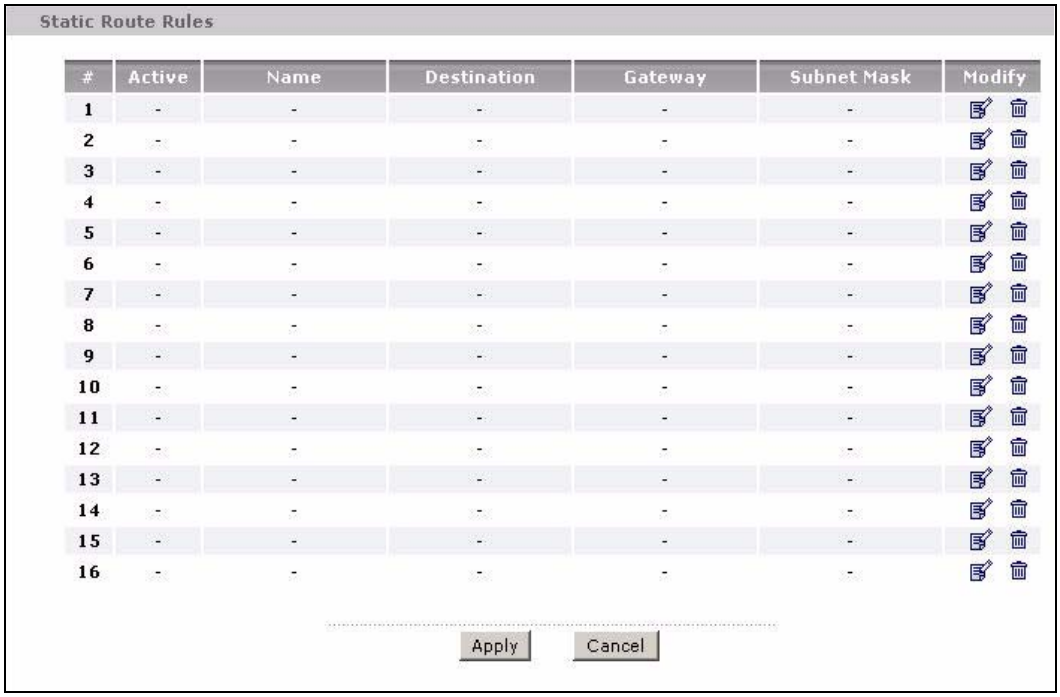
14.1.1 What You Can Do in the Static Route Screens

Use the **Static Route** screens (Section 14.2 on page 240) to view and configure IP static routes on the ZyXEL Device.

14.2 The Static Route Screen

Use this screen to view the static route rules. Click **Advanced > Static Route** to open the **Static Route** screen.

Figure 91 Advanced > Static Route



The following table describes the labels in this screen.

Table 65 Advanced > Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Name	This is the name that describes or identifies this route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the ZyXEL Device. Click the Remove icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.

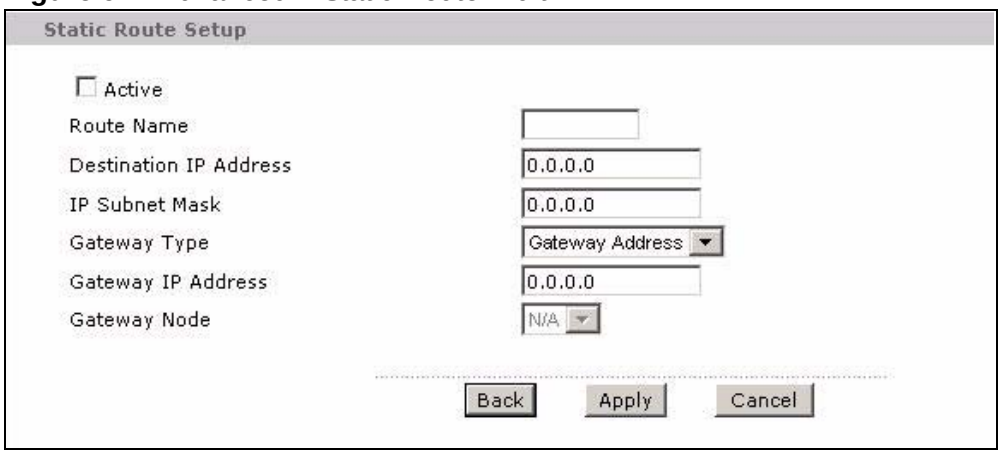
Table 65 Advanced > Static Route

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

14.2.1 Static Route Edit

Use this screen to configure the required information for a static route. Select a static route index number and click **Edit**. The screen shown next appears.

Figure 92 Advanced > Static Route: Edit



The following table describes the labels in this screen.

Table 66 Advanced > Static Route: Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Route Name	Enter the name of the IP static route. The text may consist of up to 9 letters, numerals and any printable character found on a typical English language keyboard. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway Type	Use either **Gateway Address** or **Gateway Node** to configure a static route.
Gateway IP Address	This field is available when you select **Gateway Address** from **Gateway Type**. Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.

Table 66 Advanced > Static Route: Edit

LABEL	DESCRIPTION
Gateway Node	This field is available when you select **Gateway Node** from **Gateway Type**. Select a remote node to set the static route. A remote note is a connection point outside of the local area network. One example of a remote node is your connection to your ISP. See Section 5.3 on page 95 for details on configuring a remote node.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

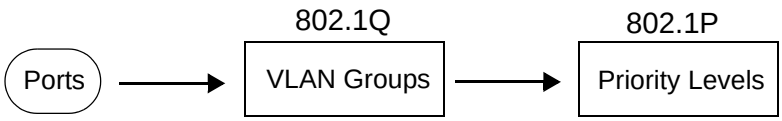
15 VLANs

15.1 Overview

This chapter describes how to configure the VLANs settings.

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. A VLAN group can be treated as an individual device. Each group can have its own rules about where and how to forward traffic. You can assign any ports on the ZyXEL Device to a VLAN group and configure the settings for the group. You may also set the priority level for traffic transmitted through the ports.

Figure 93 VLANs



15.1.1 What You Can Do in the VLANs Screens

- Use the **Group Setting** screen (Section 15.2 on page 249) to activate VLANs, specify the management VLAN group, display the VLAN groups and configure the settings for each VLAN group.
- Use the **Port Setting** screen (Section 15.3 on page 252) to configure the PVID and assign traffic priority for each port.

15.1.2 What You Need to Know About VLANs

IEEE 802.1P Priority

IEEE 802.1P specifies the user priority field and defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.

IEEE 802.1Q Tagged VLAN

Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the device on which they were created. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

PVC

A virtual circuit is a logical point-to-point circuit between customer sites. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or torn down for each session.

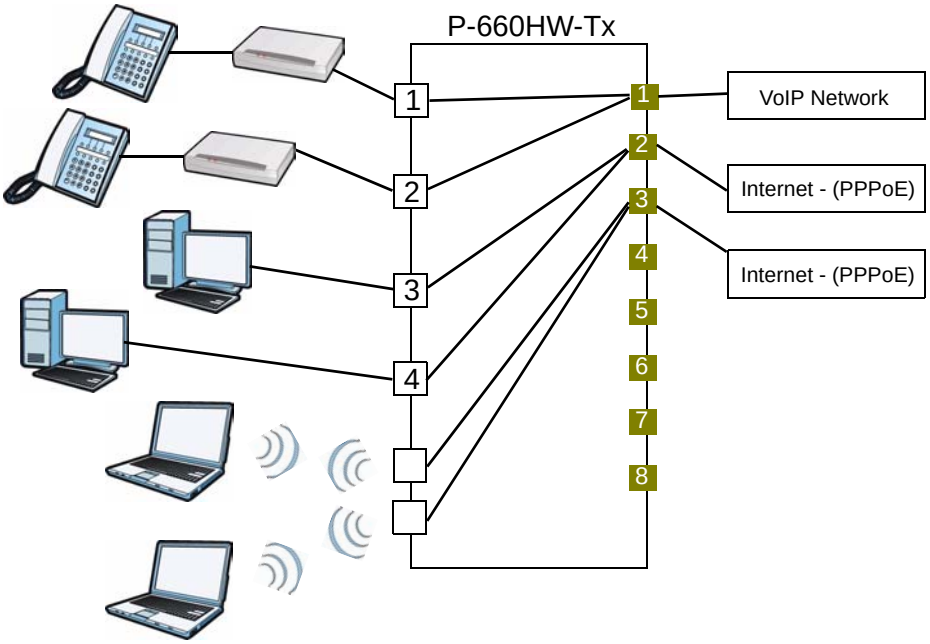
Forwarding Tagged and Untagged Frames

Each port on the device is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware device to an 802.1Q VLAN-unaware device, the ZyXEL Device first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware device to an 802.1Q VLAN-aware switch, the ZyXEL Device first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

Whether to tag an outgoing frame depends on the setting of the egress port on a per-VLAN, per-port basis (recall that a port can belong to multiple VLANs). If the tagging on the egress port is enabled for the VID of a frame, then the frame is transmitted as a tagged frame; otherwise, it is transmitted as an untagged frame.

15.1.3 VLANs Example

This example shows how to configure the VLANs settings on the ZyXEL Device.



LAN1 and LAN2 are connected to ATAs (Analogue Telephone Adapters) and used for VoIP traffic. You want to create high priority for this type of traffic, so you want to group these ports into one VLAN (VLAN2) and then to a PVC (PVC1) where the priority is set to high level of service.

You would start with the following steps.

1 Click **Advanced** > **VLANs** > **Group Setting**, and then click the **Edit** button to display the following screen.

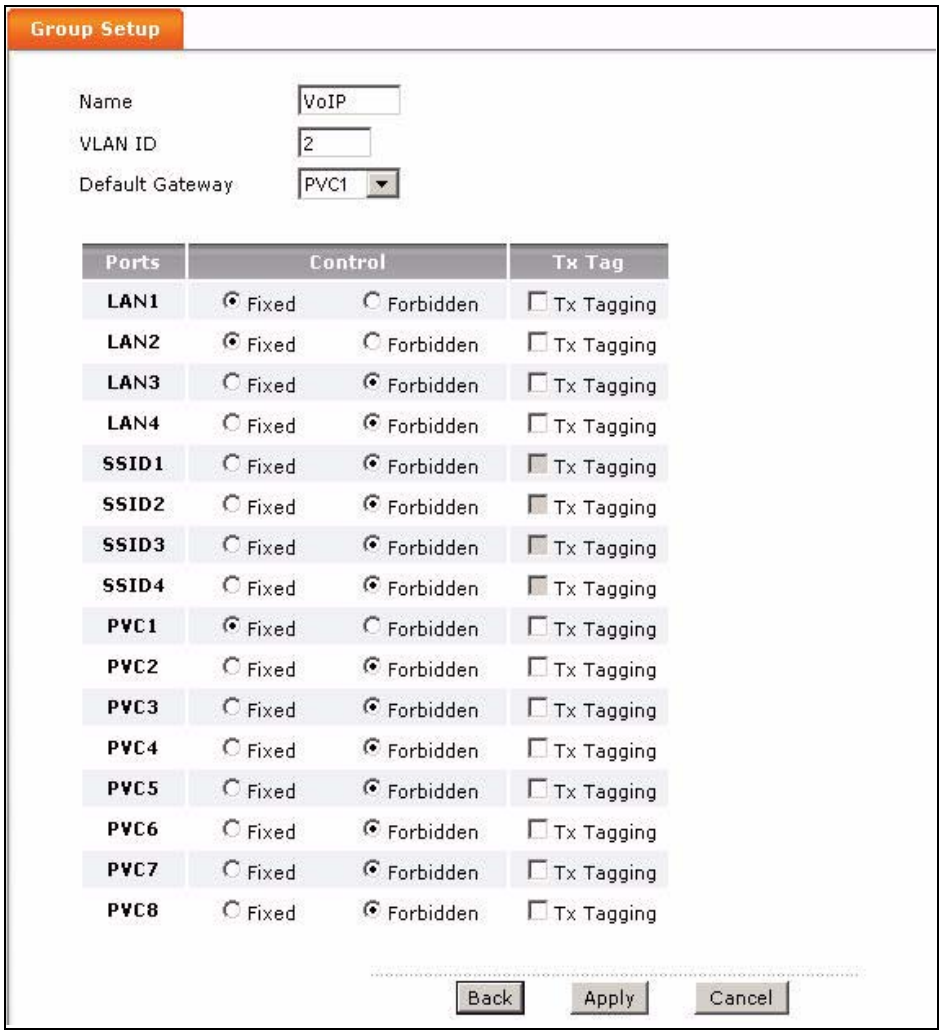
2 In the **Name** field type VoIP to identify the group.

3 In the **VLAN ID** field type in 2 to identify the VLAN group.

4 Select **PVC1** from the **Default Gateway** drop-down list box.

5 In the **Control** field, select **Fixed** for LAN1, LAN2 and PVC1 to be permanent members of the VLAN group.

6 Click **Apply**.



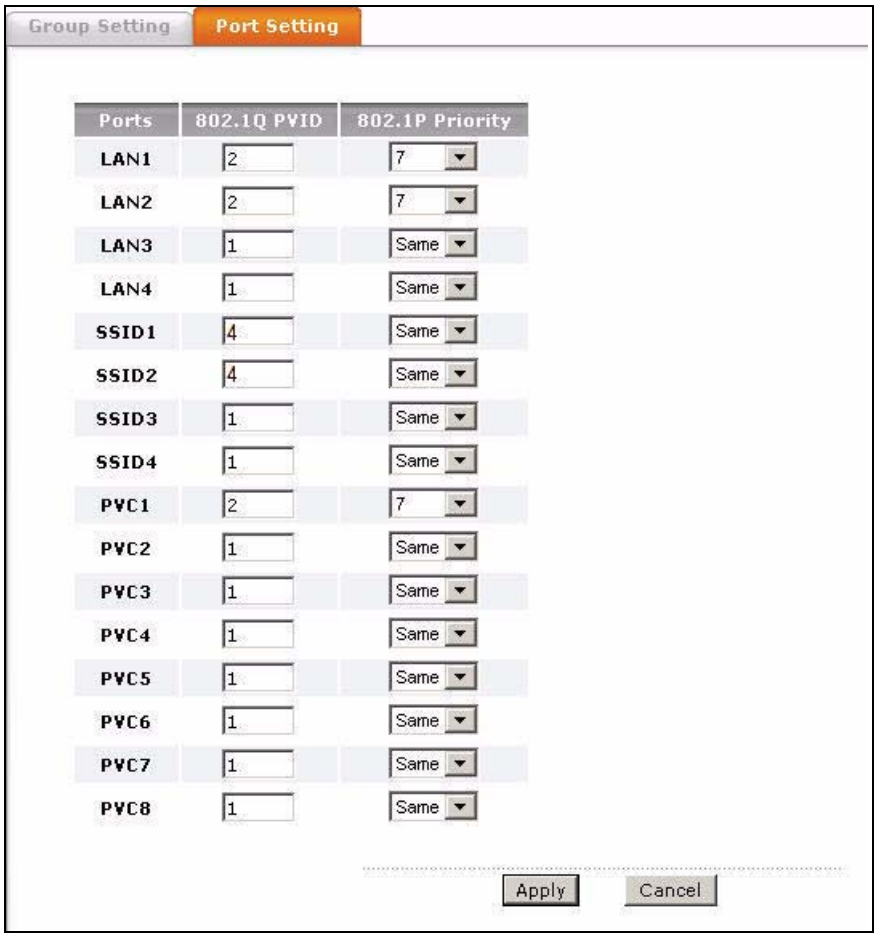
To set a high priority for VoIP traffic, follow these steps.

1 Click **Advanced** > **VLANs** > **Port Setting** to display the following screen.

2 Type 2 in the **802.1Q PVID** column for LAN1, LAN2 and PVC1.

3 Select **7** from the **802.1P Priority** drop-down list box for LAN1, LAN2 and PVC1.

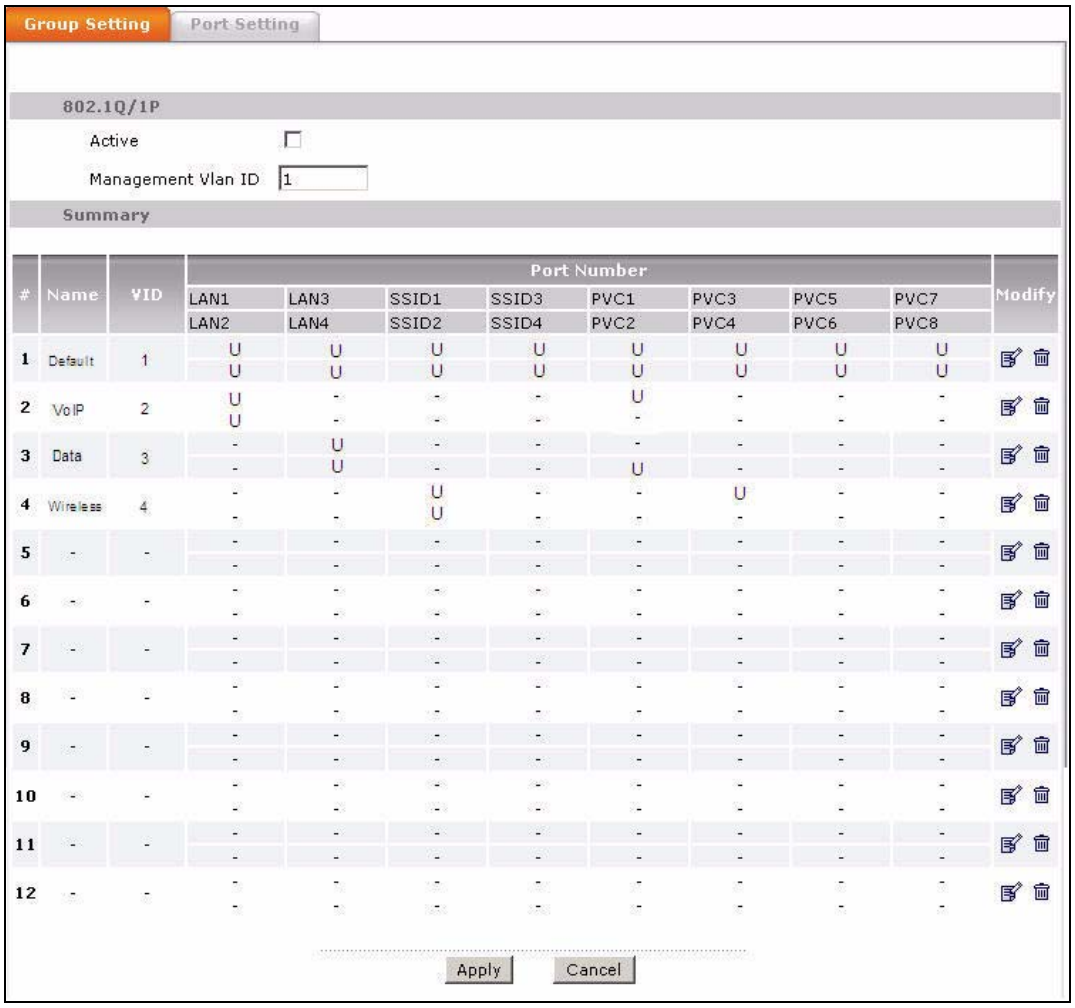
4 Click **Apply**.



Ports 3 and 4 are connected to desktop computers and are used for Internet traffic. You want to create low priority for this type of traffic, so you want to group these ports and PVC2 into one VLAN (VLAN3). PVC2 priority is set to low level of service.

SSID1 and SSID2 are two wireless networks. You want to create medium priority for this type of traffic, so you want to group these ports and PVC3 into one VLAN (VLAN4). PVC3 priority is set to medium level of service.

Follow the same steps as in VLAN2 to configure the settings for VLAN3 and VLAN4. The summary screen should then display as follows.



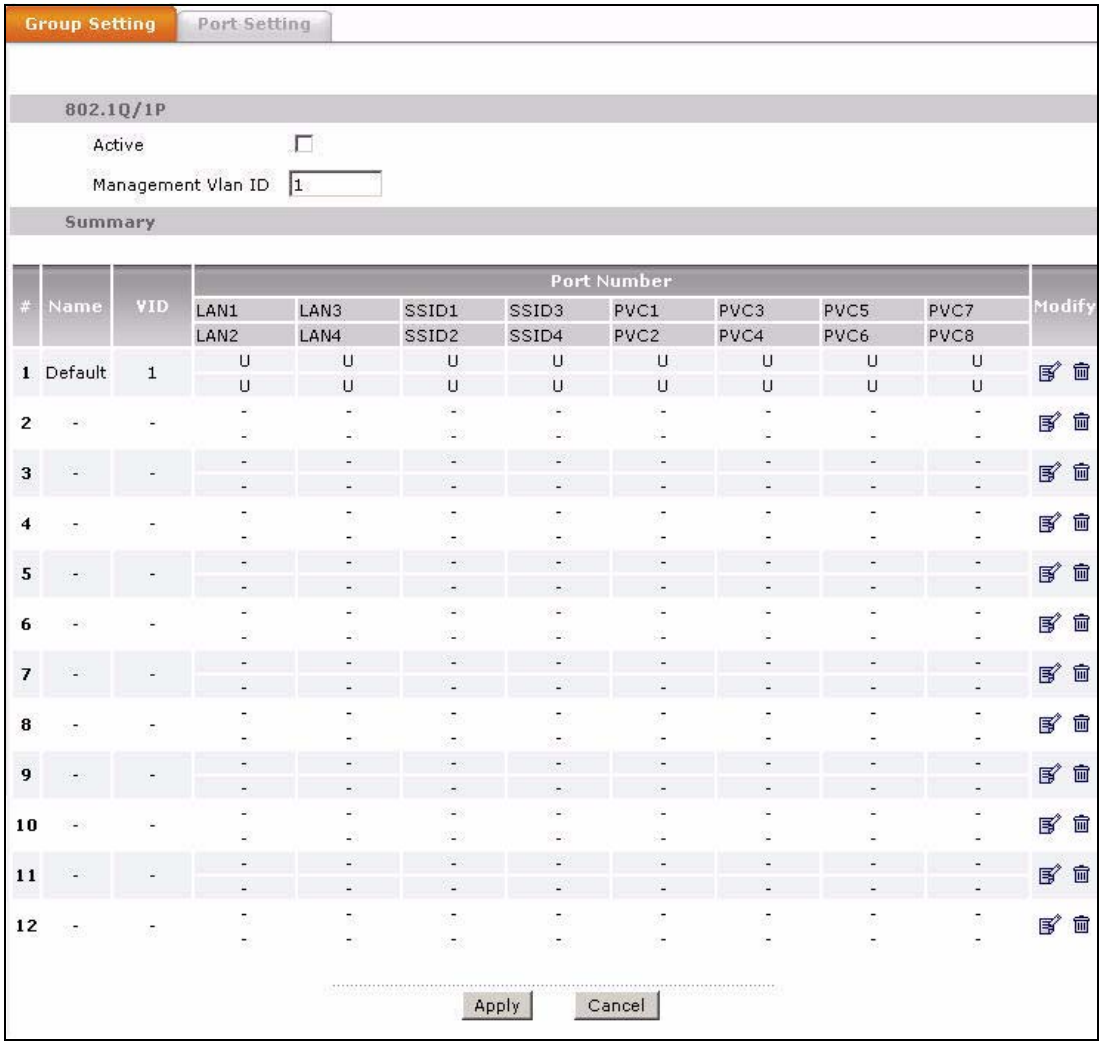
#	Name	VID	Port Number								Modify
			LAN1	LAN3	SSID1	SSID3	PVC1	PVC3	PVC5	PVC7	
			LAN2	LAN4	SSID2	SSID4	PVC2	PVC4	PVC6	PVC8	
1	Default	1	U	U	U	U	U	U	U	U	
			U	U	U	U	U	U	U	U	
2	VoIP	2	U	-	-	-	U	-	-	-	
			U	-	-	-	-	-	-	-	
3	Data	3	-	U	-	-	-	-	-	-	
			-	U	-	-	U	-	-	-	
4	Wireless	4	-	-	U	-	-	U	-	-	
			-	-	U	-	-	-	-	-	
5	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	
6	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	
7	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	
8	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	
9	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	
10	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	
11	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	
12	-	-	-	-	-	-	-	-	-	-	
			-	-	-	-	-	-	-	-	

This completes the VLANs setup.

15.2 The VLANs Group Setting Screen

Use this screen to activate 802.1Q/1P and display the VLAN groups. Click **Advanced > VLANs** to display the following screen.

Figure 94 Advanced > VLANs > Group Setting



The following table describes the labels in this screen.

Table 67 Advanced > VLANs > Group Setting

LABEL	DESCRIPTION
802.1Q/1P	
Active	Select this check box to activate the 802.1P/1Q feature.
Management Vlan ID	Enter the ID number of a VLAN group. All interfaces (ports, SSIDs and PVCs) are in the management VLAN by default. If you disable the management VLAN, you will not be able to access the ZyXEL Device.
Summary	
#	This field displays the index number of the VLAN group.

Table 67 Advanced > VLANs > Group Setting (continued)

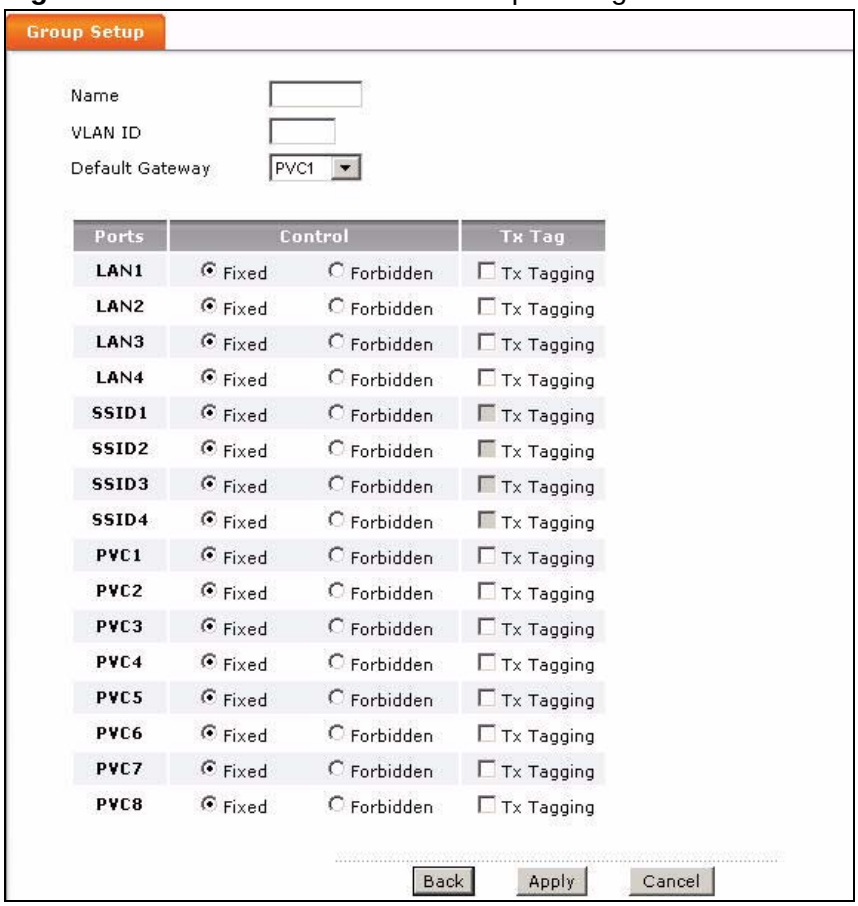
LABEL	DESCRIPTION
Name	This field displays the name of the VLAN group.
VID	This field displays the ID number of the VLAN group.
Port Number	These columns display the VLAN's settings for each port. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN are marked as "**–**".
Modify	Click the **Edit** button to configure the ports in the VLAN group. Click the **Remove** button to delete the VLAN group.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

15.2.1 Editing VLANs Group Setting

Use this screen to configure the settings for each VLAN group.

In the **VLANs** screen, click the **Edit** button from the **Modify** filed to display the following screen.

Figure 95 Advanced > VLANs > Group Setting > Edit



The following table describes the labels in this screen.

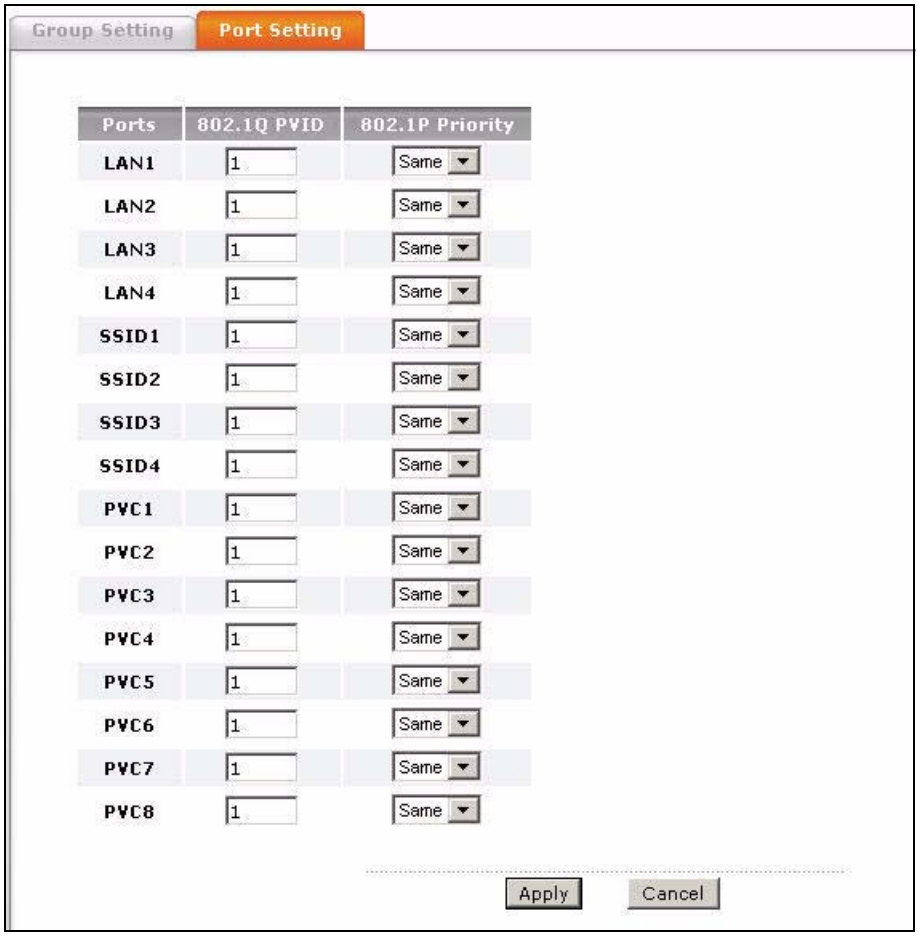
Table 68 Advanced > 802.1Q/1P > Group Setting > Edit

LABEL	DESCRIPTION
Name	Enter a descriptive name for the VLAN group for identification purposes. The text may consist of up to 8 letters, numerals, “-”, “_” and “@”.
VLAN ID	Assign a VLAN ID for the VLAN group. The valid VID range is between 1 and 4094.
Default Gateway	Select the default gateway for the VLAN group.
Ports	This field displays the types of ports available to join the VLAN group.
Control	Select **Fixed** for the port to be a permanent member of the VLAN group. Select **Forbidden** if you want to prohibit the port from joining the VLAN group.
Tx Tag	Select **Tx Tagging** if you want the port to tag all outgoing traffic transmitted through this VLAN. You select this if you want to create VLANs across different devices and not just the ZyXEL Device.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

15.3 The VLANs Port Setting Screen

Use this screen to configure the PVID and assign traffic priority for each port. Click **Advanced** > **VLANs** > **Port Setting** to display the following screen.

Figure 96 Advanced > VLANs > Port Setting



The following table describes the labels in this screen.

Table 69 Advanced > VLANs > Port Setting

LABEL	DESCRIPTION
Ports	This field displays the types of ports available to join the VLAN group.
802.1Q PVID	Assign a VLAN ID for the port. The valid VID range is between 1 and 4094. The ZyXEL Device assigns the PVID to untagged frames or priority-tagged frames received on this port.
802.1P Priority	Assign a priority for the traffic transmitted through the port. Select **Same** if you do not want to modify the priority. You may choose a priority level from **0-7**, with 0 being the lowest level and 7 being the highest level.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

16

Quality of Service (QoS)

16.1 Overview

Use the **QoS** screens to set up your ZyXEL Device to use QoS for traffic management.

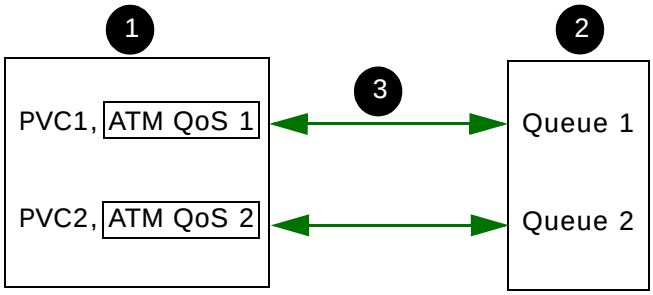
Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control bandwidth. QoS allows the ZyXEL Device to group and prioritize application traffic and fine-tune network performance.

Without QoS, all traffic data are equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as video-on-demand.

The ZyXEL Device assigns each packet a priority and then queues the packet accordingly. Packets assigned with a high priority are processed more quickly than those with low priorities if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

16.2 QoS Overview

The following figure gives an overview of how to configure QoS on this ZyXEL Device:



1 First, you have to configure WAN connection(s) in **Network > Internet (WAN) > Internet Access Setup** and **Network > Internet (WAN) > More Connections**. Click the **Advanced Setup** button on the corresponding PVC setting screens to configure ATM QoS, if you want to prioritize traffic and eliminate congestion over the ATM network (at the ATM layer).

2 Configure queue settings in **Advanced > QoS > Queue Setup** according to the priority you want to apply to different types of traffic.

3 Configure class settings in **Advanced > QoS > Class Setup**. This associates queues with PVCs by mapping the priority of queues to the index number of PVCs.

16.2.1 What You Can Do in the QoS Screens

- Use the **General** screen (Section 16.3 on page 259) to enable QoS on the ZyXEL Device, decide allowable bandwidth using QoS and configure priority mapping settings for traffic that does not match a custom class.
- Use the **Class Setup** screen (Section 16.4 on page 260) to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow.
- Use the **Queue Setup** screen (Section 16.7.1 on page 267) to configure QoS queue assignment.
- Use the **Monitor** screen (Section 16.7.1 on page 267) to view the ZyXEL Device's QoS-related packet statistics.

16.2.2 What You Need to Know About QoS

QoS versus CoS

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. Class of Service (CoS) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

CoS technologies include IEEE 802.1p layer 2 tagging and Differentiated Services (DiffServ or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit Type of Service (ToS) field in the IP header.

Tagging and Marking

In a QoS class, you can configure whether to add or change the DiffServ Code Point (DSCP) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

Finding Out More

See Section 16.8 on page 270 for advanced technical information on QoS.

16.2.3 QoS Class Setup Example

In the following figure, your Internet connection has an upstream transmission speed of 50 Mbps. You configure a classifier to assign the priority queue (5) to VoIP traffic from the LAN interface, so that voice traffic would not get delayed when there is network congestion. Traffic from the boss's IP address (192.168.1.23 for example) is mapped to queue 4. Traffic that does not match

these two classes are assigned priority queue based on the internal QoS mapping table on the ZyXEL Device.

Figure 97 QoS Example

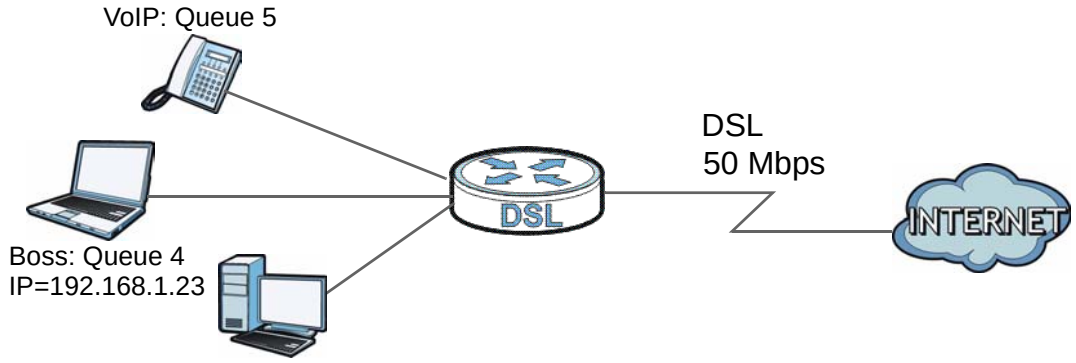


Figure 98 QoS Class Example: VoIP -1

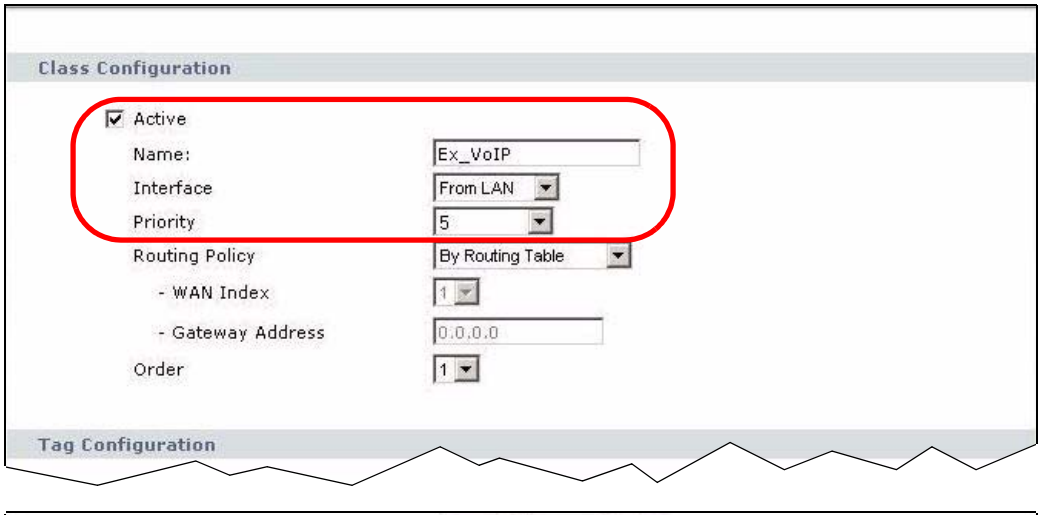


Figure 99 QoS Class Example: VoIP -2

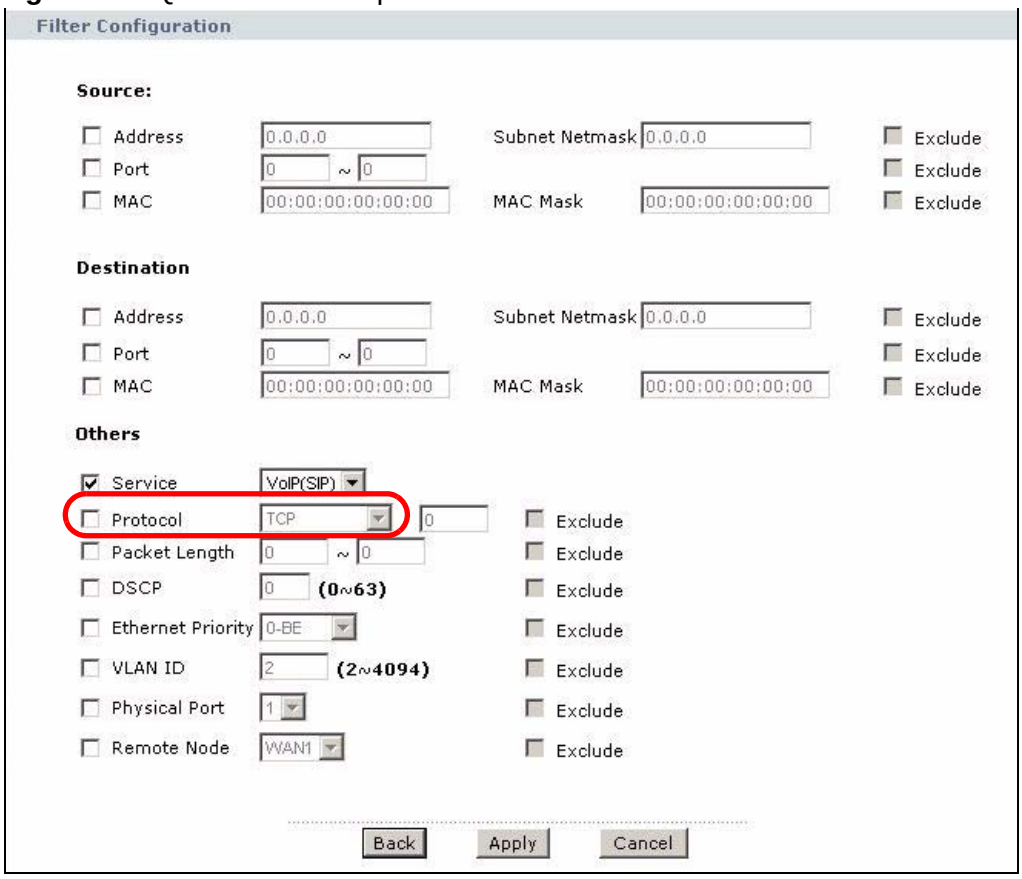


Figure 100 QoS Class Example: Boss -1

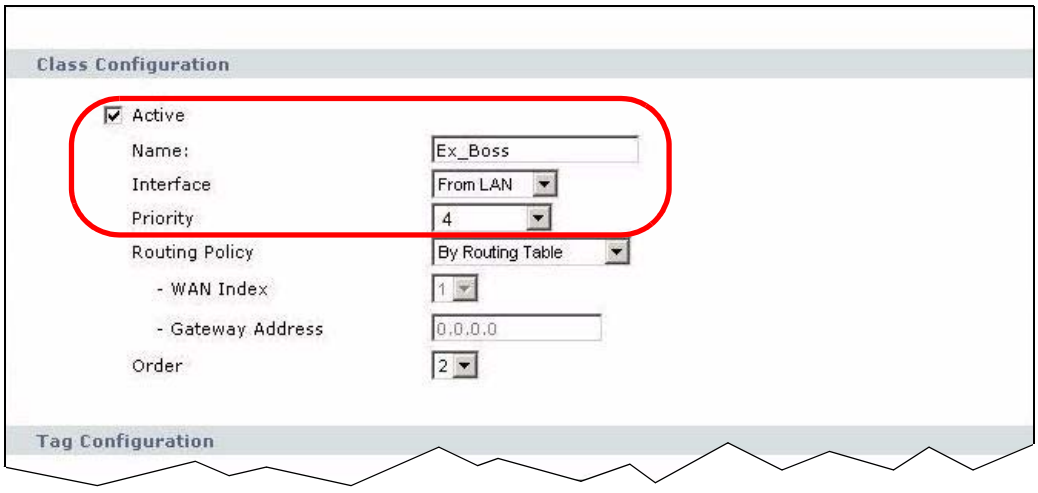
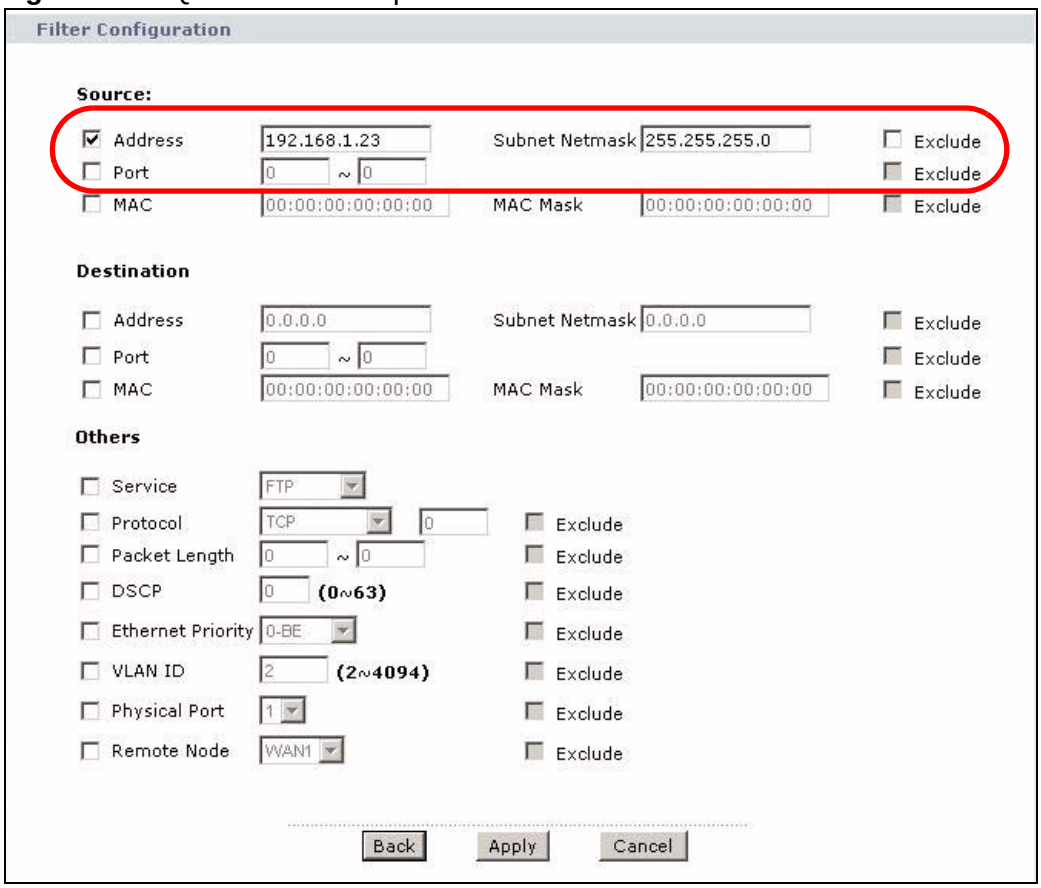


Figure 101 QoS Class Example: Boss -2

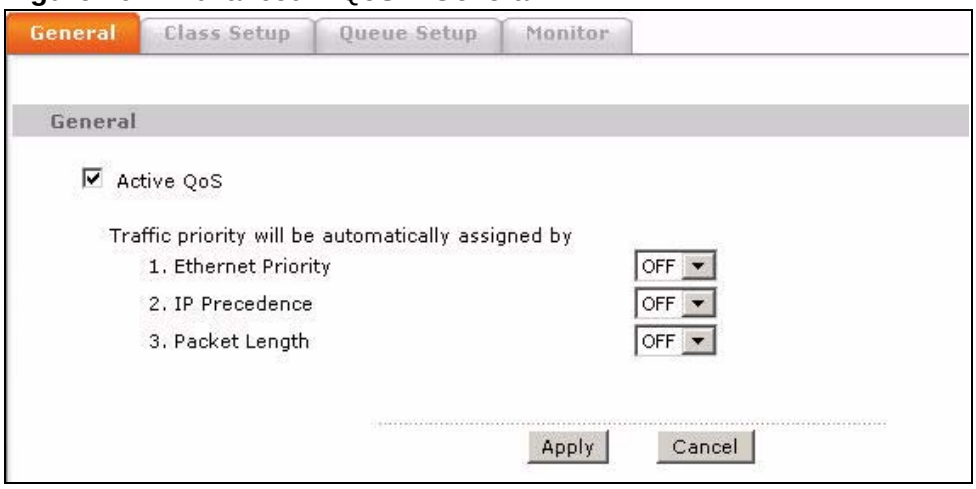


16.3 The QoS General Screen

Use this screen to enable or disable QoS and have the ZyXEL Device automatically assign priority to traffic according to the IEEE 802.1p priority level, IP precedence and/or packet length.

Click **Advanced > QoS** to open the screen as shown next.

Figure 102 Advanced > QoS > General



The following table describes the labels in this screen.

Table 70 Advanced > QoS > General

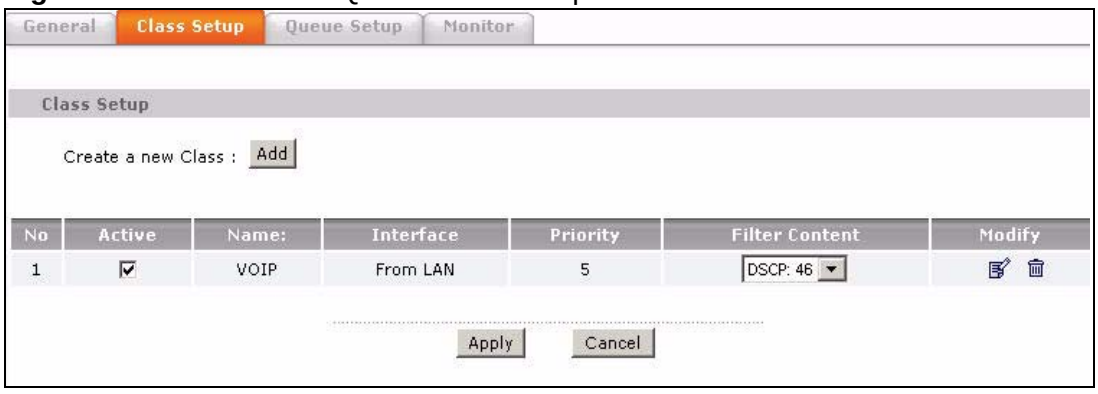
LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance. You can give priority to traffic that the ZyXEL Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
Traffic priority will be automatically assigned by	These fields are ignored if traffic matches a class you configured in the **Class Setup** screen. If you select **ON** and traffic does not match a class configured in the **Class Setup** screen, the ZyXEL Device assigns priority to unmatched traffic based on the IEEE 802.1p priority level, IP precedence and/or packet length. See Section 16.8.4 on page 272 for more information. If you select **OFF**, traffic which does not match a class is mapped to queue two.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

16.4 The Class Setup Screen

Use this screen to add, edit or delete classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Click **Advanced > QoS > Class Setup** to open the following screen.

Figure 103 Advanced > QoS > Class Setup



The following table describes the labels in this screen.

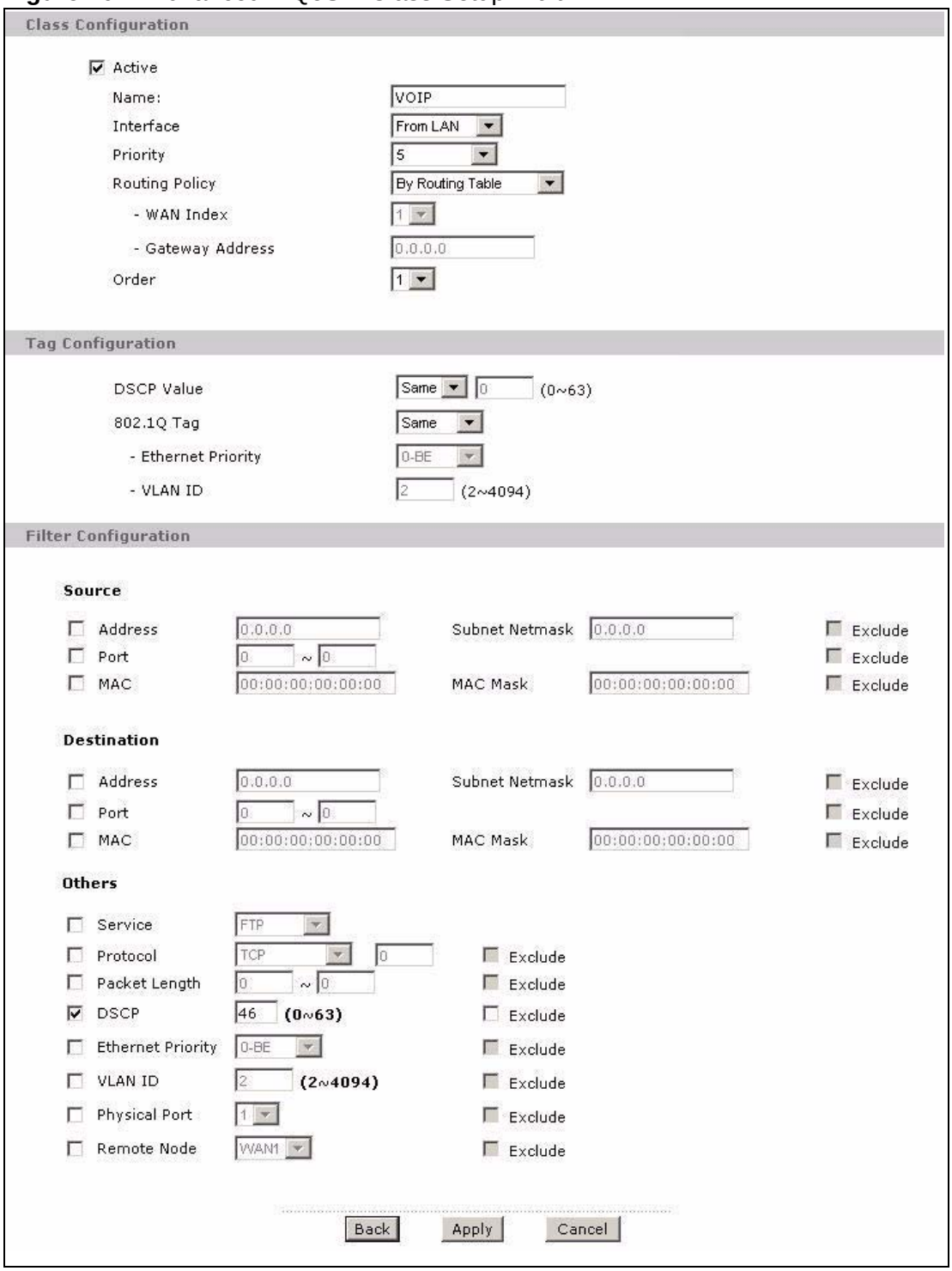
Table 71 Advanced > QoS > Class Setup

LABEL	DESCRIPTION
Create a new Class	Click this to create a new classifier.
No	This is the number of each classifier. The ordering of the classifiers is important as the classifiers are applied in turn.
Active	Select the check box to enable this classifier.
Name	This is the name of the classifier.
Interface	This shows the interface from which traffic of this classifier should come.
Priority	This is the priority assigned to traffic of this classifier.
Filter Content	This shows criteria specified in this classifier.
Modify	Click the Edit icon to go to the screen where you can edit the classifier. Click the Remove icon to delete an existing classifier.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

16.4.1 The Class Configuration Screen

Use this screen to configure a classifier. Click the **Add** button or the **Edit** icon in the **Modify** field to display the following screen.

Figure 104 Advanced > QoS > Class Setup: Edit



See Appendix E on page 421 for a list of commonly-used services. The following table describes the labels in this screen.

Table 72 Advanced > QoS > Class Setup: Edit

LABEL	DESCRIPTION
Class Configuration	
Active	Select the check box to enable this classifier.
Name	The text may consist of up to 20 letters, numerals and any printable character found on a typical English language keyboard.
Interface	Select from which interface traffic of this class should come.
Priority	Select a priority level (between 0 and 7) or select **Auto** to have the ZyXEL Device map the matched traffic to a queue according to the internal QoS mapping table. See Section 16.8.4 on page 272 for more information. "0" is the lowest priority level and "7" is the highest.
Routing Policy	Select the next hop to which traffic of this class should be forwarded. Select **By Routing Table** to have the ZyXEL Device use the routing table to find a next hop and forward the matched packets automatically. Select **To WAN Index** to route the matched packets through the specified PVC. This option is available only when the WAN type is ADSL. Select **To Gateway Address** to route the matched packets to the router or switch you specified in the **Gateway Address** field.
WAN Index	Select a PVC index number.
Gateway Address	Enter the IP address of the gateway, which should be a router or switch on the same segment as the ZyXEL Device's interface(s), that can forward the packet to the destination.
Order	This shows the ordering number of this classifier. Select an existing number for where you want to put this classifier and click **Apply** to move the classifier to the number you selected. For example, if you select 2, the classifier you are moving becomes number 2 and the previous classifier 2 gets pushed down one.
Tag Configuration	
DSCP Value	Select **Same** to keep the DSCP fields in the packets. Select **Auto** to map the DSCP value to 802.1 priority level automatically. Select **Mark** to set the DSCP field with the value you configure in the field provided.

Table 72 Advanced > QoS > Class Setup: Edit (continued)

LABEL	DESCRIPTION
802.1Q Tag	Select **Same** to keep the priority setting and VLAN ID of the frames. Select **Auto** to map the 802.1 priority level to the DSCP value automatically. Select **Remove** to delete the priority queue tag and VLAN ID of the frames. Select **Mark** to replace the 802.1 priority field and VLAN ID with the value you set in the fields below. Select **Add** to treat all matched traffic untagged and add a second priority queue tag and VLAN.
Ethernet Priority	Select a priority level (between 0 and 7) from the drop down list box.
VLAN ID	Specify a VLAN ID number between 2 and 4094.
Filter Configuration	Use the following fields to configure the criteria for traffic classification.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	Enter the source subnet mask. Refer to the appendix for more information on IP subnetting.
Port	Select the check box and enter the port number of the source. 0 means any source port number. See Appendix E on page 421 for some common services and port numbers.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the destination IP address in dotted decimal notation.
Subnet Netmask	Enter the destination subnet mask. Refer to the appendix for more information on IP subnetting.
Port	Select the check box and enter the port number of the destination. 0 means any source port number. See Appendix E on page 421 for some common services and port numbers.
MAC	Select the check box and enter the destination MAC address of the packet.

Table 72 Advanced > QoS > Class Setup: Edit (continued)

LABEL	DESCRIPTION
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified destination MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
Service	This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields. SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select the check box and select **VoIP(SIP)** from the drop-down list box to configure this classifier for traffic that uses SIP. File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. Select the check box and select **FTP** from the drop-down list box to configure this classifier for FTP traffic.
Protocol	Select this option and select the protocol (**TCP** or **UDP**) or select **User defined** and enter the protocol (service type) number. 0 means any protocol number.
Packet Length	Select this option and enter the minimum and maximum packet length (from 28 to 1500) in the fields provided.
DSCP	Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
Ethernet Priority	Select this option and select a priority level (between 0 and 7) from the drop down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	Select this option and specify a VLAN ID number between 2 and 4094.
Physical Port	Select this option and select a LAN port.
Remote Node	Select this option and select a remote node from the drop down list box. When the WAN type is **Ethernet** in the **Internet (WAN) > Internet Access Setup** screen, you can select **WAN1** only.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

16.5 Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or queues). Token Bucket is a traffic shaping algorithm that allows a certain amount of large bursts while keeping a limit at the average rate. Your ZyXEL Device uses the Token Bucket algorithm.

16.6 Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket is a buffer that temporarily stores outgoing packets and transmits them at an average rate. The algorithm allows bursts of up to *b* bytes which is also the bucket size.

In your ZyXEL Device, each token represents 1 byte, so the bucket can hold up to *b* tokens. A token is generated and added into the bucket every 1/t seconds. If a *b+1* token arrives (a token that arrives after the bucket is full), that token will be discarded. The following shows how tokens work with outgoing packets:

- A packet can be transmitted if the number of tokens in the bucket are equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, the number of tokens that correspond to the packet size are removed from the bucket.
- If there are no tokens in the bucket, the ZyXEL Device stops transmitting until enough tokens are generated.
- If not enough tokens are available, the ZyXEL Device treats the packet in either one of the following ways:
  - Drops it.
  - Holds it in the queue until enough tokens are available in the bucket.
  - Transmits it but adds a mark. The ZyXEL Device may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface's capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger shaping rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

16.7 Token Bucket Example

This is an example of how the token bucket works.

Table 73 Example Data

b=125,000 bytes (around 1 Megabit)	This is the size of the bucket. The bucket holds up to 125,000 tokens.
t=100	This means a token is generated every 0.01 (=1/t) seconds. The maximum instantaneous transmission rate for outgoing traffic is (b'x8)/t Mbps where b' is the number of tokens in the bucket at that instant.

The algorithm works as follows (see also Figure 105 on page 266):

A: Assume that there are 2000 tokens in the bucket at the first moment (T = 0).

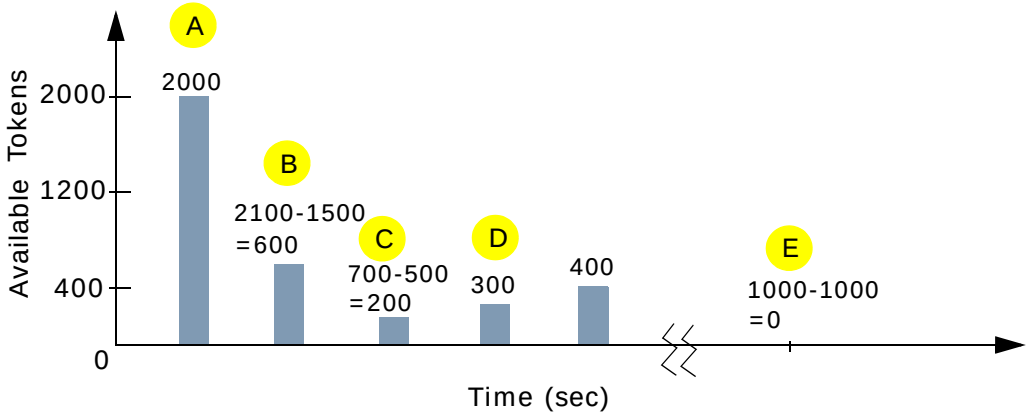
B: One hundred tokens are added to the bucket after one second. A packet of 1500 bytes arrives and the ZyXEL Device transmits it directly as there are already enough tokens in the bucket to cover the size of the packet. The ZyXEL Device then deducts 1500 tokens from the bucket leaving 600 tokens in the bucket (2100-1500).

C: One hundred more tokens are added in the bucket after one second. A packet of 500 bytes arrives and the ZyXEL Device again transmits it directly and then deducts 500 tokens from the bucket leaving just 200 tokens (700-500).

D: After one more second, one hundred more tokens are added to the bucket. A packet of 1000 bytes flows in. The ZyXEL Device holds the packet since the number of tokens are insufficient.

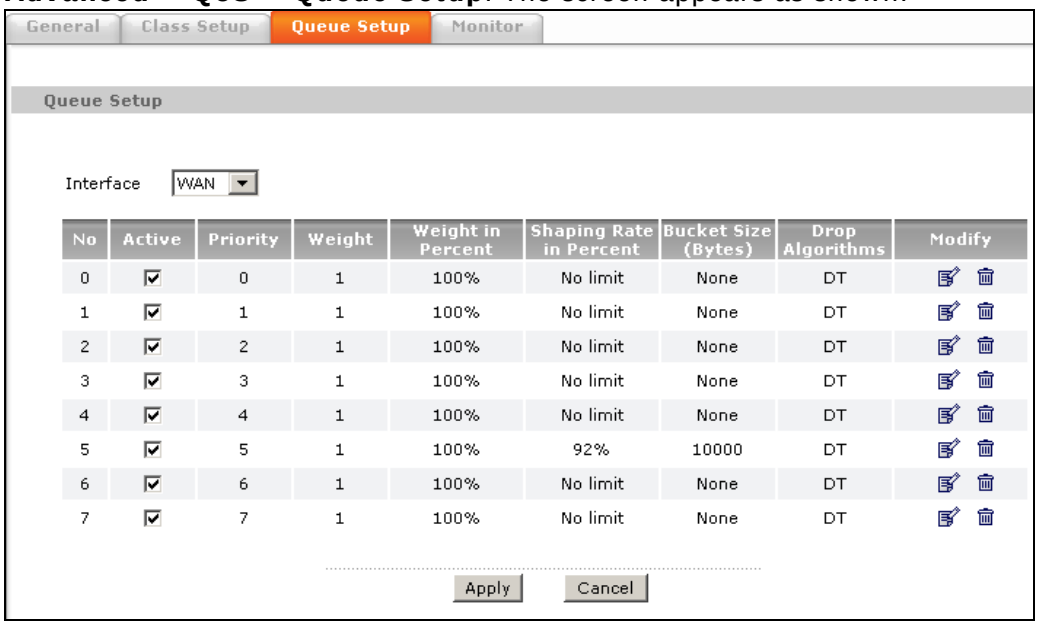
E: After enough tokens (1000) are in the bucket, the ZyXEL Device transmits it and then deducts 1000 tokens from the bucket.

Figure 105 Token Bucket Scenario Example



16.7.1 The Queue Setup Screen

Use this screen to view or modify the ZyXEL Device's Queue Setup. Click **Advanced > QoS > Queue Setup**. The screen appears as shown.



The following table describes the labels in this screen.

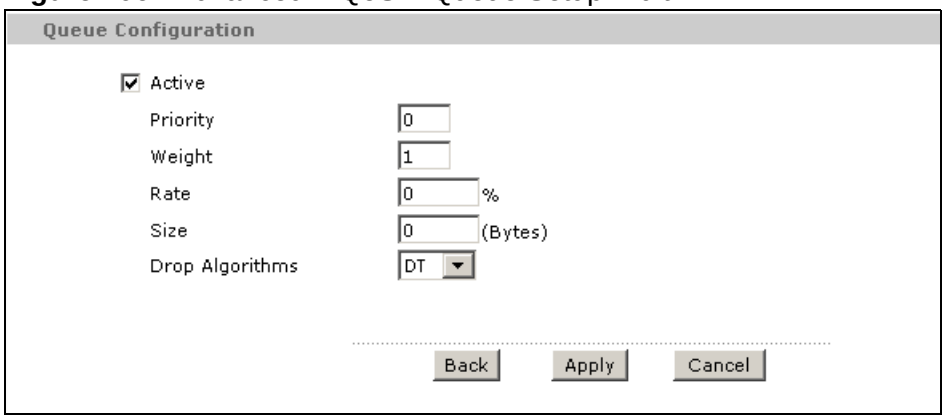
Table 74 QoS Queue Setup

LABEL	DESCRIPTION
Interface	Select through which interface traffic of this queue should go.
No.	This is the index number of this entry.
Active	Select the check box to enable the queue.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Weight in Percent	This shows the weight of this queue in percentage of all queues with the same priority.
Shaping Rate in Percent	This shows the maximum transmission rate allowed for traffic on this queue.
Bucket Size(Bytes)	This shows the size of the bucket, which is the maximum amount of bytes that tokens can be available for instantaneously.
Drop Algorithms	This shows the queue management algorithm used for this queue.
Modify	Click the **Edit** icon to go to the screen where you can edit the queue. Click the **Remove** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16.7.2 The Queue Configuration Screen

Use this screen to configure a queue. Click the **Edit** icon in the **Modify** field to display the following screen.

Figure 106 Advanced > QoS > Queue Setup: Edit



The following table describes the labels in this screen.

Table 75 QoS Queue Setup: Edit

LABEL	DESCRIPTION
Class Configuration	
Active	Select the check box to enable this queue.
Priority	Specify the priority level (from 0 to 7) of this queue. The higher the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Specify the weight (from 1 to 8) of this queue. If two queues have the same priority level, the ZyXEL Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Rate	Specify the maximum transmission rate allowed for traffic on this queue. If you select **WAN** as the interface in the **Advanced > QoS > Queue Setup** screen, the rate is in percentage of the total bandwidth. If you select **LAN** or **WLAN** as the interface, the rate is the maximum transmission rate in kpbs.
Size	Specify the token bucket size (in bytes) on this queue. The size range is from 1,500 to 100,000 bytes and the maximum transmission rate must be set if you want to configure the bucket size. You can refer to Section 16.6 on page 265 for more information on Token Bucket.

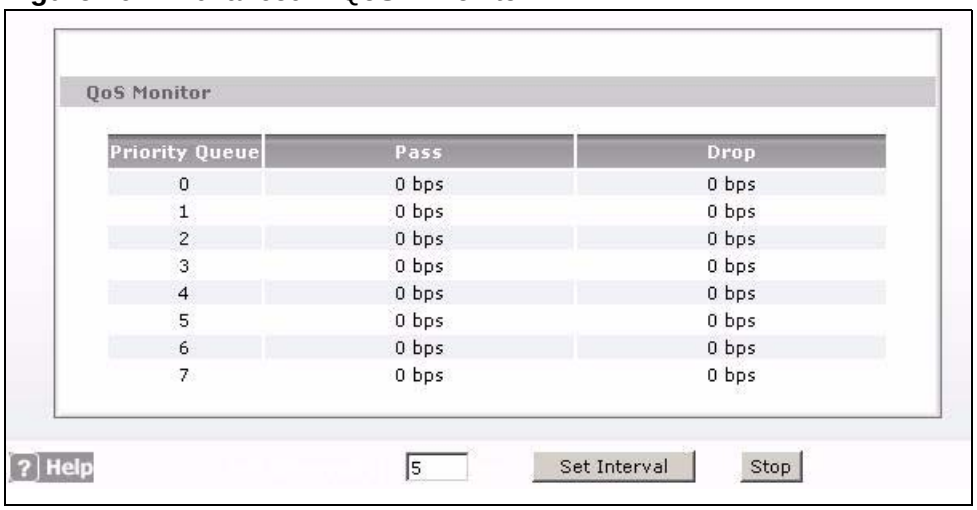
Table 75 QoS Queue Setup: Edit (continued)

LABEL	DESCRIPTION
Drop Algorithms	Queue management algorithms determine how the ZyXEL Device should handle packets when it receives too many (network congestion). **Drop Tail (DT)** is a simple queue management algorithm that allows the ZyXEL Device buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it). **Random Early Detection (RED)** is a queue management algorithm that doesn't wait until a buffer is full before dropping packets. If the buffer is almost empty, all incoming packets are accepted. As the queue grows, the probability for dropping an incoming packet grows too. When the buffer is full, the probability has reached 1 and all incoming packets are dropped. Select RED if your network is usually congested and/or has much bursty traffic.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16.7.3 The QoS Monitor Screen

Use this screen to view the ZyXEL Device's QoS packet statistics. Click **Advanced > QoS > Monitor**. The screen appears as shown.

Figure 107 Advanced > QoS > Monitor



The following table describes the labels in this screen.

Table 76 Advanced > QoS > Monitor

LABEL	DESCRIPTION
Priority Queue	This shows the priority queue number. Traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.
Pass	This shows how many packets mapped to this priority queue are transmitted successfully.
Drop	This shows how many packets mapped to this priority queue are dropped.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click this to stop refreshing statistics.

16.8 QoS Technical Reference

This section provides some technical background information about the topics covered in this chapter.

16.8.1 IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 77 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.

Table 77 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

16.8.2 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

16.8.3 DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

Differentiated Services (DiffServ) is a Class of Service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new Differentiated Services (DS) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

16.8.4 Automatic Priority Queue Assignment

If you enable QoS on the ZyXEL Device, the ZyXEL Device can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the ZyXEL Device. On the ZyXEL Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 78 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	

Table 78 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

17

Dynamic DNS Setup

17.1 Overview

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

17.1.1 What You Can Do in the DDNS Screen

Use the **Dynamic DNS** screen (Section 17.2 on page 276) to enable DDNS and configure the DDNS settings on the ZyXEL Device.

17.1.2 What You Need To Know About DDNS

DYNDNS Wildcard

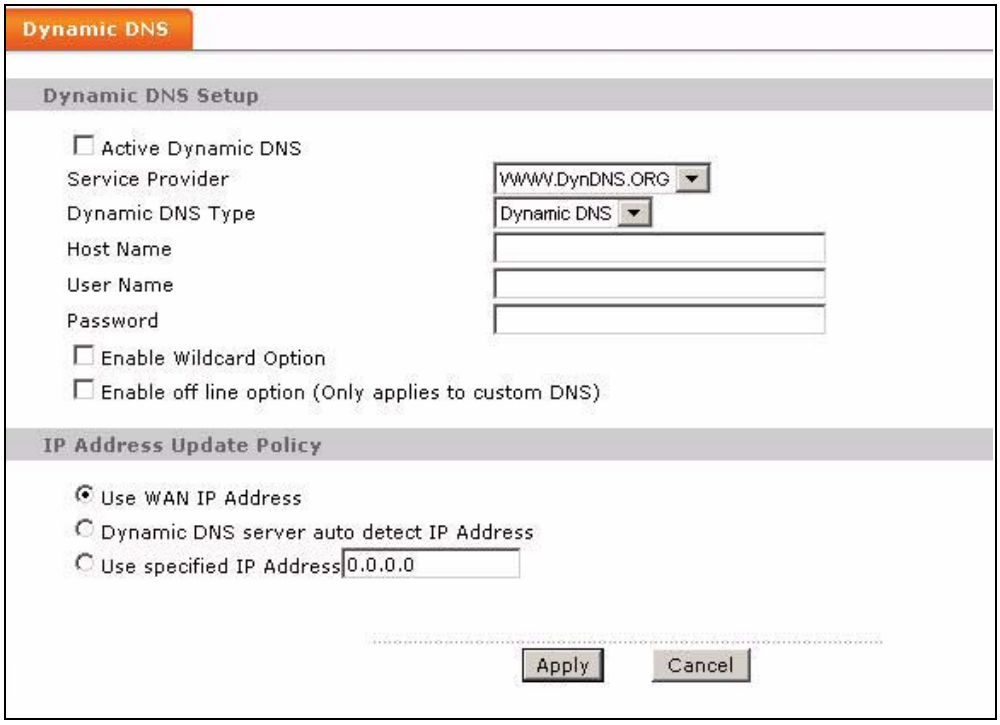
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

17.2 The Dynamic DNS Screen

Use this screen to change your ZyXEL Device's DDNS. Click **Advanced > Dynamic DNS**. The screen appears as shown.

Figure 108 Advanced > Dynamic DNS



The following table describes the fields in this screen.

Table 79 Advanced > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.

Table 79 Advanced > Dynamic DNS (continued)

LABEL	DESCRIPTION
Enable off line option	This option is available when **CustomDNS** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.
Dynamic DNS server auto detect IP Address	Select this option only when there are one or more NAT routers between the ZyXEL Device and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyXEL Device and the DDNS server.
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

18

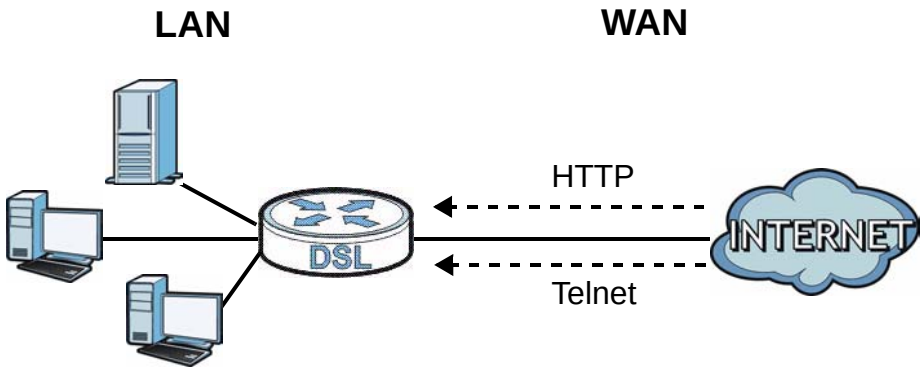
Remote Management

18.1 Overview

Remote management allows you to determine which services/protocols can access which ZyXEL Device interface (if any) from which computers.

The following figure shows remote management of the ZyXEL Device coming in from the WAN.

Figure 109 Remote Management From the WAN



Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

You may manage your ZyXEL Device from a remote location via:

- Internet (WAN only)
- LAN only
- WLAN only
- LAN and WAN
- LAN and WLAN
- WLAN and WAN
- ALL (WAN, LAN and WLAN)
- None (Disable)

You may only have one remote management session running at a time. The ZyXEL Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1 Telnet

2 HTTP

18.1.1 What You Can Do in the Remote Management Screens

- Use the **WWW** screen (Section 18.2 on page 281) to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the ZyXEL Device.
- Use the **Telnet** screen (Section 18.3 on page 284) to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyXEL Device.
- Use the **FTP** screen (Section 18.4 on page 285) to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyXEL Device.
- Use the **DNS** screen (Section 18.5 on page 286) to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyXEL Device.
- Use the **ICMP** screen (Section 18.6 on page 287) to set whether or not your ZyXEL Device will respond to pings and probes for services that you have not made available.

18.1.2 What You Need to Know About Remote Management

Remote Management Limitations

Remote management does not work when:

- You have not enabled that service on the interface in the corresponding remote management screen.
- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- There is a firewall rule that blocks it.

Remote Management and NAT

When NAT is enabled:

- Use the ZyXEL Device's WAN IP address when configuring from the WAN.
- Use the ZyXEL Device's LAN IP address when configuring from the LAN.

System Timeout

There is a default system management idle timeout of 15 minutes (900 seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

18.2 The WWW Screen

To enable Remote Management from the WAN for web access you have two options: create a dynamic firewall rule or manually create a firewall rule. The dynamic firewall rule is the simplest but unlike the manual firewall rule option it does not allow you to specify the source IP address(es) for WAN access.

18.2.0.1 Creating Dynamic WWW rule

1 Click **Advanced** > **Remote MGMT** > **WWW** and set **Access Status** to **ALL** (or **LAN & WAN** or **WLAN & WAN**).

Note: IMPORTANT! If you choose WAN it will ONLY allow access from the WAN.

2 Next click on the option **Create a dynamic firewall rule** to permit WAN access and click the **Apply** button.

To disable WAN remote management for Web, simply reverse the above. Be careful to set the **Access Status** to either or both **LAN** and **WLAN**.

Note: It is recommended if you are allowing WAN access even temporarily to change the default password (in **Maintenance** > **System** > **General**).

18.2.0.2 Manual WWW Rule

1 Click **Advanced** > **Remote MGMT** > **WWW** and set **Access Status** to **ALL** (or **LAN & WAN** or **WLAN & WAN**).

Note: IMPORTANT! If you choose WAN it will ONLY allow access from the WAN.

2 Next click on the Firewall link in Note3 of the screen. For WAN access: If you want to specify the source IP address for remote management, click on the Firewall link. This will then redirect you to the main Firewall screen (**Security** >**Firewall** > **General**).

3 Here you will choose the **Custom** option (please note that the Custom option will inherit the default firewall behaviour of the firewall option that was specified previously (**High** or **Medium**, BUT NOT for **Low** as it blocks WAN to LAN access but this can easily be changed).

4 Next go to the **Rules** tab and in **Packet direction** choose **WAN to WAN/Router**. Click the **Add** button.

5 In the Edit rule page that appears you may want to change the source address from **Any**. Otherwise in **Service** > **selected services** remove **Any(TCP)** and **Any(UDP)** and move **HTTP(TCP:80)** from available services to **selected services**. Now click on the **Apply** button.

Note: it is recommended if you are allowing WAN access even temporarily to change the default password (in Maintenance > System > General). In the New Password box, type in a new password (up to 30 characters). Retype it in the Retype to confirm box. Then click Apply to save your changes. Use the new password to login.

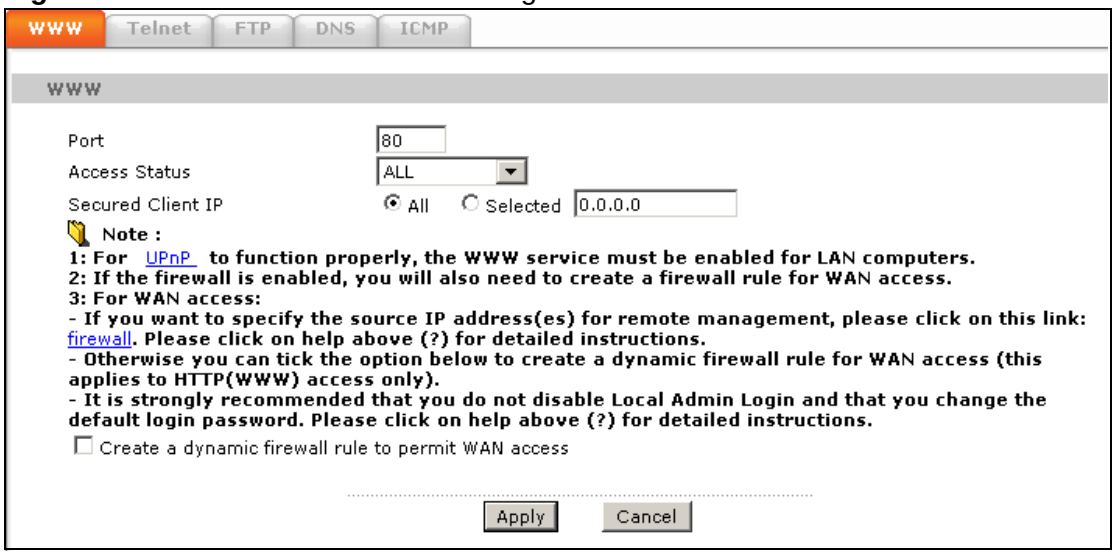
Use this screen to specify how to connect to the ZyXEL Device from a web browser, such as Internet Explorer.

Note: If you disable the **WWW** service in the **Remote MGMT > WWW** screen, then the ZyXEL Device blocks all HTTP connection attempts.

18.2.1 Configuring the WWW Screen

Click **Advanced > Remote MGMT** to display the **WWW** screen.

Figure 110 Advanced > Remote Management > WWW


WWW
Telnet
FTP
DNS
ICMP
WWW
Port
80
Access Status
ALL
Secured Client IP
All
Selected
0.0.0.0
Note :
1: For UPnP to function properly, the WWW service must be enabled for LAN computers.
2: If the firewall is enabled, you will also need to create a firewall rule for WAN access.
3: For WAN access:
- If you want to specify the source IP address(es) for remote management, please click on this link: firewall. Please click on help above (?) for detailed instructions.
- Otherwise you can tick the option below to create a dynamic firewall rule for WAN access (this applies to HTTP(WWW) access only).
- It is strongly recommended that you do not disable Local Admin Login and that you change the default login password. Please click on help above (?) for detailed instructions.
Create a dynamic firewall rule to permit WAN access
Apply
Cancel

The following table describes the labels in this screen.

Table 80 Advanced > Remote Management > WWW

LABEL	DESCRIPTION
Port	You may change the server port number for a service, if needed. However, you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Create a dynamic firewall rule to permit WAN access	Select this check box if you want to create a dynamic firewall rule to permit WAN access. This option is available only when you set the **Access Status** as **ALL**, **WAN**, **WLAN&WAN**, or **LAN&WAN**.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

18.3 The Telnet Screen

You can use Telnet to access the ZyXEL Device's command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

To enable Remote Management from the WAN for Telnet access:

1 Go to **Advanced** > **Remote MGMT** > **Telnet** and set **Access Status** to **ALL** (or **WAN & LAN** or **WAN & WLAN**).

Note: IMPORTANT! If you choose WAN it will ONLY allow access from the WAN.

2 Next click on the Firewall link in Note3 of the screen. For WAN access: If you want to specify the source IP address for remote management, click on the Firewall link. This will then redirect you to the main Firewall screen (**Security** >**Firewall** > **General**).

3 Here you will choose the **Custom** option (please note that the Custom option will inherit the default firewall behaviour of the firewall option that was specified previously (**High** or **Medium**, BUT NOT for **Low** as it blocks WAN to LAN access but this can easily be changed).

4 Next go to the **Rules** tab and in **Packet direction** choose **WAN to WAN/Router**. Click the **Add** button.

5 In the Edit rule page that appears you may want to change the source address from **Any**. Otherwise in **Service** > **selected services** remove **Any(TCP)** and **Any(UDP)** and move **Telnet(TCP:23)** from available services to selected services. Now click on the **Apply** button.

Note: it is recommended if you are allowing WAN access even temporarily to change the default password (in **Maintenance** > **System** > **General**).

To remove Telnet remote management:

1 Go to **Advanced** > **Remote MGMT** > **Telnet** and set **Access Status** to **LAN**, **WLAN**, **WLAN & LAN** or **Disabled**.

2 Next go to **Security** > **Firewall** > **General**. There will be a **Rules** tab if **Custom** is specified as the firewall option.

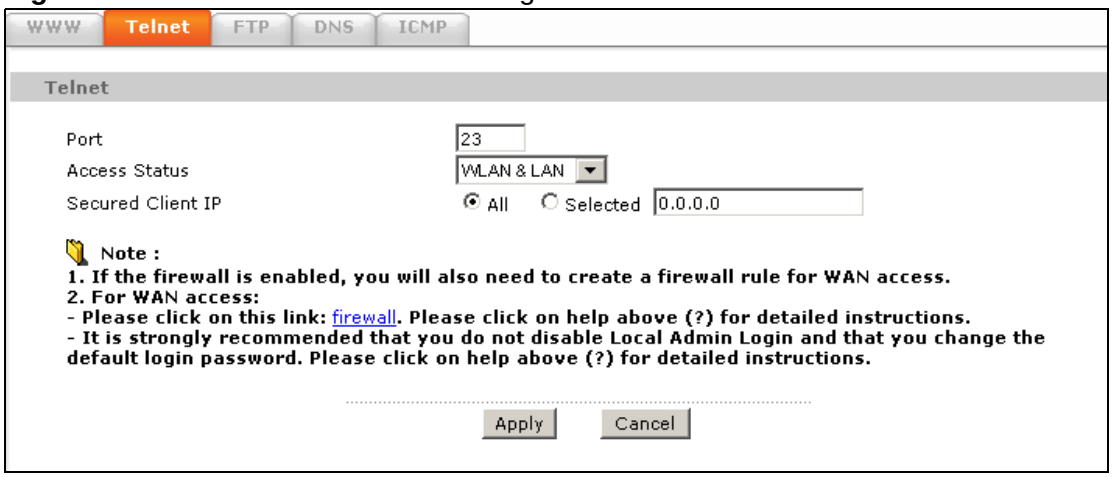
3 In **Packet direction** choose **WAN to WAN/Router**.

4 Untick the Active tick box for your remote management rule and click the **Apply** button.

Note: it is recommended if you are allowing WAN access even temporarily to change the default password (in Maintenance > System > General). In the New Password box, type in a new password (up to 30 characters). Retype it in the Retype to confirm box. Then click Apply to save your changes. Use the new password to login.

Click **Advanced > Remote MGMT** > **Telnet** tab to display the screen as shown.

Figure 111 Advanced > Remote Management > Telnet


WWW
Telnet
FTP
DNS
ICMP
Telnet
Port
23
Access Status
WLAN & LAN
Secured Client IP
All
Selected
0.0.0.0
Note :
1. If the firewall is enabled, you will also need to create a firewall rule for WAN access.
2. For WAN access:
- Please click on this link: firewall. Please click on help above (?) for detailed instructions.
- It is strongly recommended that you do not disable Local Admin Login and that you change the default login password. Please click on help above (?) for detailed instructions.
Apply
Cancel

The following table describes the labels in this screen.

Table 81 Advanced > Remote Management > Telnet

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

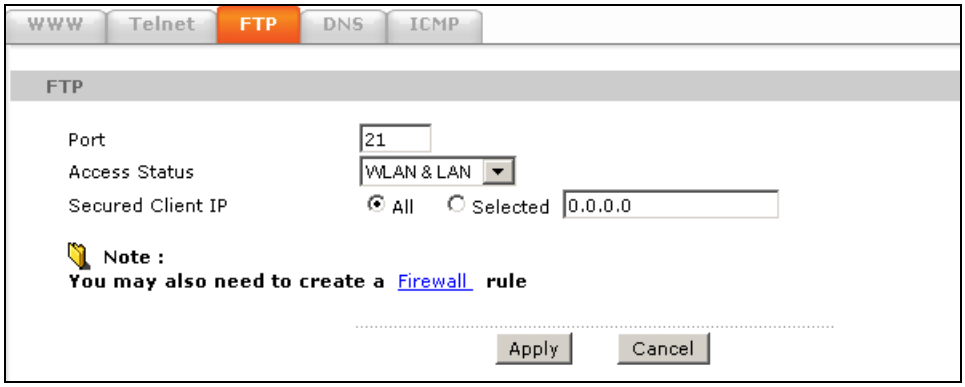
18.4 The FTP Screen

You can use FTP (File Transfer Protocol) to upload and download the ZyXEL Device’s firmware and configuration files. Please see the User’s Guide chapter on

firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

Use this screen to specify which interfaces allow FTP access and from which IP address the access can come. To change your ZyXEL Device's FTP settings, click **Advanced > Remote MGMT** > **FTP**. The screen appears as shown.

Figure 112 Advanced > Remote Management > FTP



The following table describes the labels in this screen.

Table 82 Advanced > Remote Management > FTP

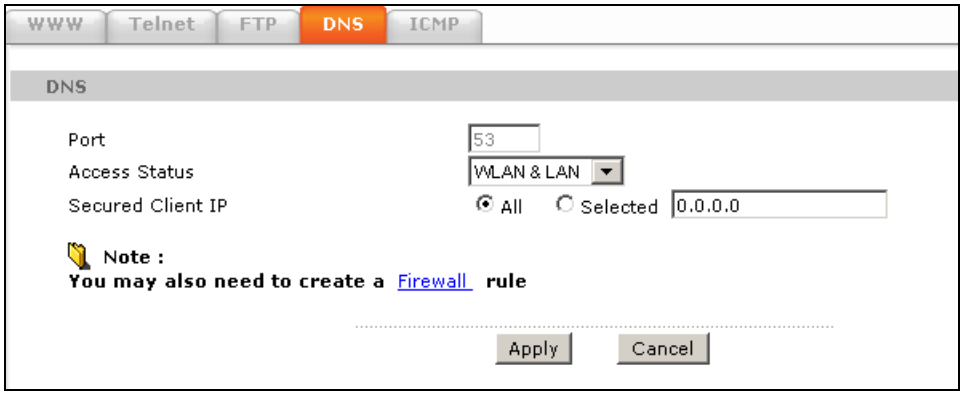
LABEL	DESCRIPTION
Port	You may change the server port number for a service, if needed. However, you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

18.5 The DNS Screen

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to Chapter 6 on page 111 for background information.

Use this screen to set from which IP address the ZyXEL Device will accept DNS queries and on which interface it can send them your ZyXEL Device's DNS settings. This feature is not available when the ZyXEL Device is set to bridge mode. Click **Advanced > Remote MGMT** > **DNS** to change your ZyXEL Device's DNS settings.

Figure 113 Advanced > Remote Management > DNS



The following table describes the labels in this screen.

Table 83 Advanced > Remote Management > DNS

LABEL	DESCRIPTION
Port	The DNS service port number is 53 and cannot be changed here.
Access Status	Select the interface(s) through which a computer may send DNS queries to the ZyXEL Device.
Secured Client IP	A secured client is a "trusted" computer that is allowed to send DNS queries to the ZyXEL Device. Select **All** to allow any computer to send DNS queries to the ZyXEL Device. Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the ZyXEL Device.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

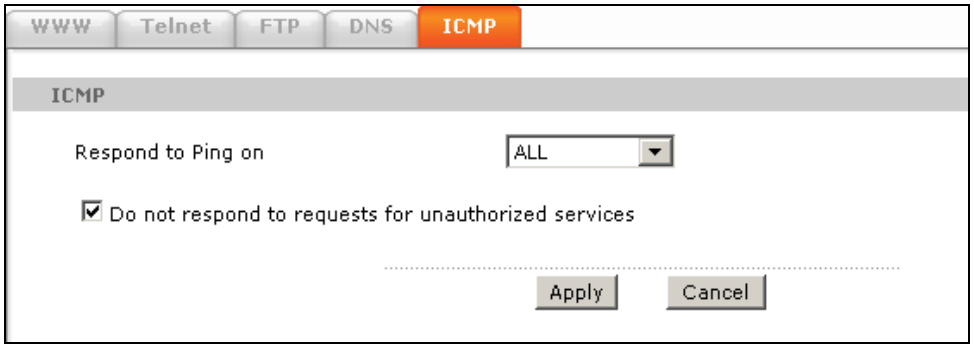
18.6 The ICMP Screen

To change your ZyXEL Device's security settings, click **Advanced > Remote MGMT** > **ICMP**. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. Your ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

Note: If you want your device to respond to pings and requests for unauthorized services, you may also need to configure the firewall anti probing settings to match.

Figure 114 Advanced > Remote Management > ICMP



The following table describes the labels in this screen.

Table 84 Advanced > Remote Management > ICMP

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The ZyXEL Device will not respond to any incoming Ping requests when **Disable** is selected. Select **ALL** to reply to all incoming Ping requests. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to both incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the ZyXEL Device by probing for unused ports. If you select this option, the ZyXEL Device will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyXEL Device unseen. If this option is not selected, the ZyXEL Device will reply with an ICMP port unreachable packet for a port probe on its unused UDP ports and a TCP reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the ZyXEL Device's firewall rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the ZyXEL Device reacts based on the firewall rule to either send a TCP reset packet for a blocked TCP packet (or an ICMP port-unreachable packet for a blocked UDP packets) or just drop the packets without sending a response packet.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

19

Universal Plug-and-Play (UPnP)

19.1 Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

19.1.1 What You Can Do in the UPnP Screen

Use the **UPnP** screen (Section 19.2 on page 291) to enable UPnP on the ZyXEL Device and allow UPnP-enabled applications to automatically configure the ZyXEL Device.

19.1.2 What You Need to Know About UPnP

Identifying UPnP Devices

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyXEL Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

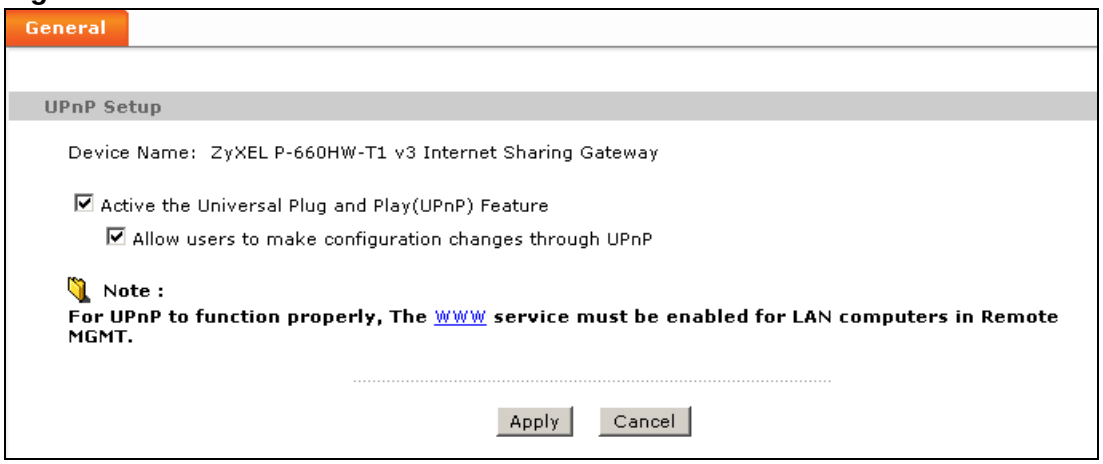
See the following sections for examples of installing and using UPnP.

19.2 The UPnP Screen

Use the following screen to configure the UPnP settings on your ZyXEL Device. Click **Advanced > UPnP** to display the screen shown next.

See Section 19.1 on page 289 for more information.

Figure 115 Advanced > UPnP > General


General
UPnP Setup
Device Name: ZyXEL P-660HW-T1 v3 Internet Sharing Gateway
Active the Universal Plug and Play(UPnP) Feature
Allow users to make configuration changes through UPnP
Note :
For UPnP to function properly, The WWW service must be enabled for LAN computers in Remote MGMT.
Apply
Cancel

The following table describes the fields in this screen.

Table 85 Advanced > UPnP > General

LABEL	DESCRIPTION
Active the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyXEL Device so that they can communicate through the ZyXEL Device, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

19.3 Installing UPnP in Windows Example

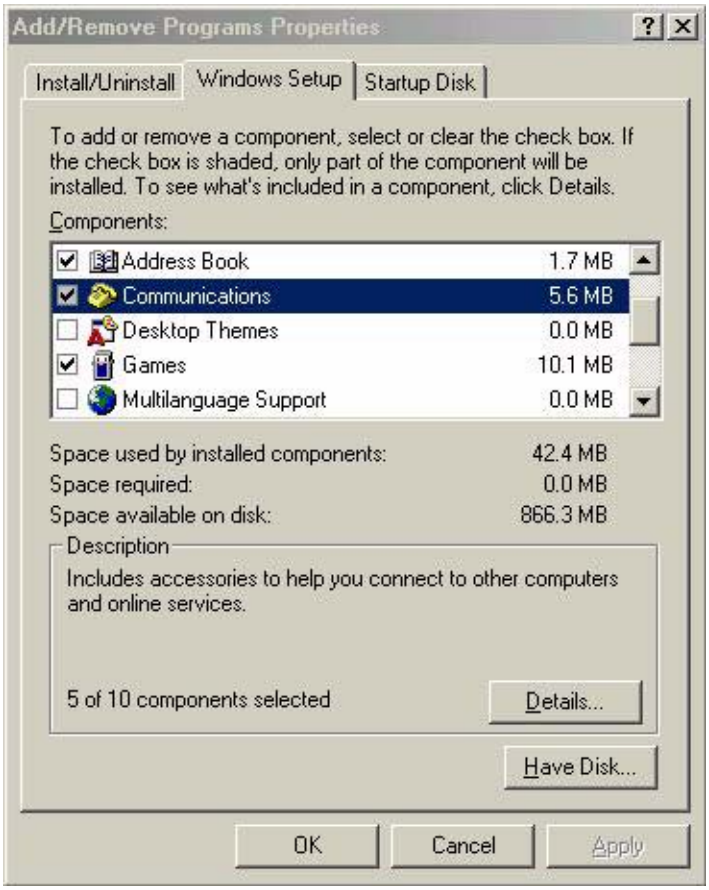
This section shows how to install UPnP in Windows Me and Windows XP.

Installing UPnP in Windows Me

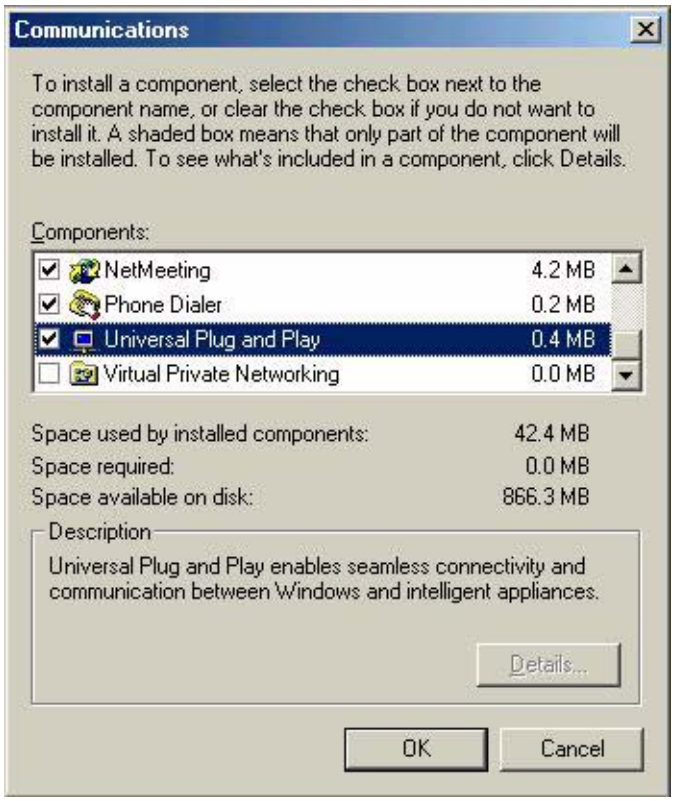
Follow the steps below to install the UPnP in Windows Me.

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.


Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.
Components:
Address Book 1.7 MB
Communications 5.6 MB
Desktop Themes 0.0 MB
Games 10.1 MB
Multilanguage Support 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Includes accessories to help you connect to other computers and online services.
5 of 10 components selected
Details...
Have Disk...
OK
Cancel
Apply

3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.


Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 4.2 MB
Phone Dialer 0.2 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Installing UPnP in Windows XP

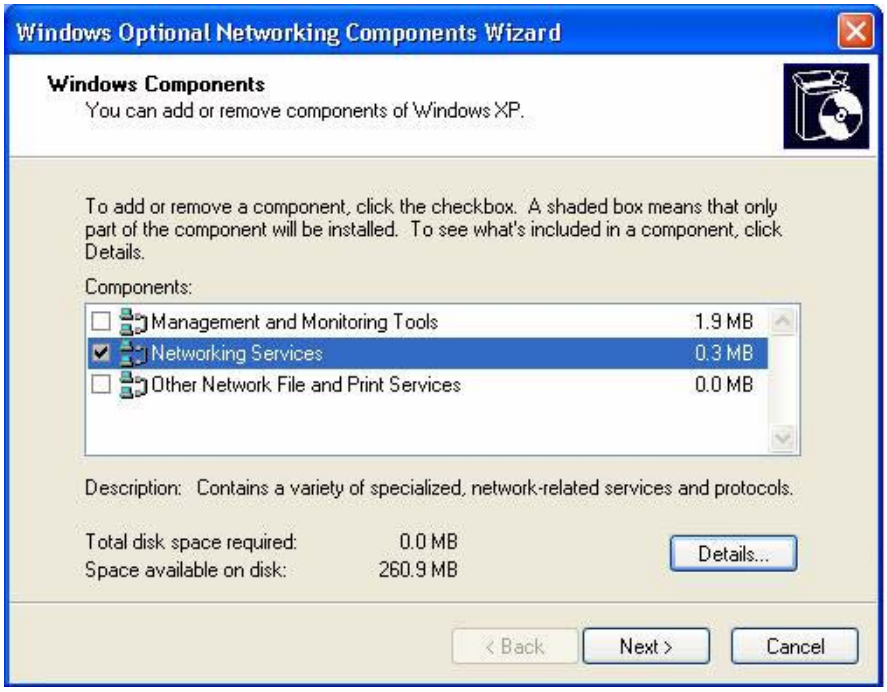
Follow the steps below to install the UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

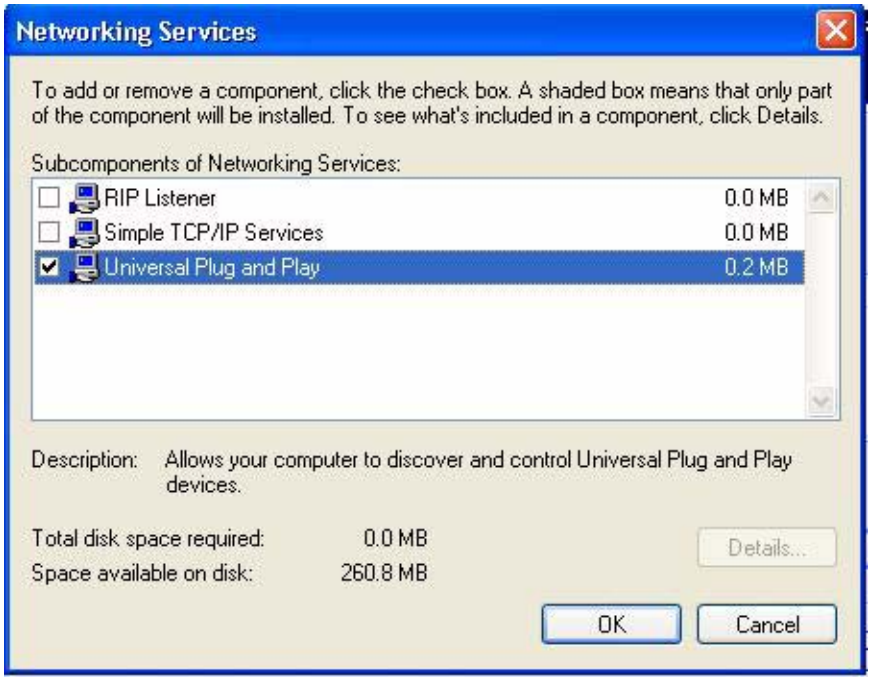
2 Double-click **Network Connections**.

3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 1.9 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 260.9 MB
Details...
< Back
Next >
Cancel

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Allows your computer to discover and control Universal Plug and Play devices.
Total disk space required: 0.0 MB
Space available on disk: 260.8 MB
Details...
OK
Cancel

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

19.4 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL Device.

Make sure the computer is connected to a LAN port of the ZyXEL Device. Turn on your computer and the ZyXEL Device.

Auto-discover Your UPnP-enabled Network Device

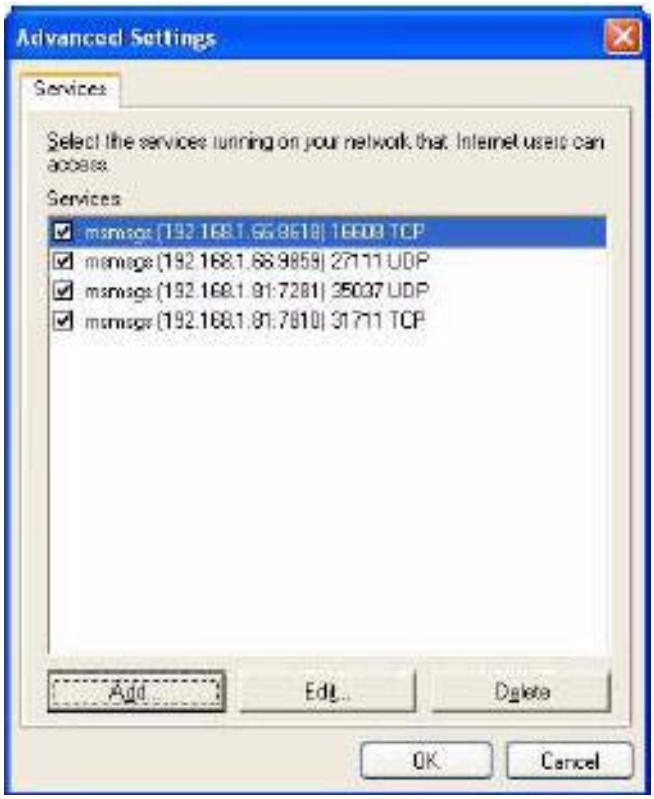
1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

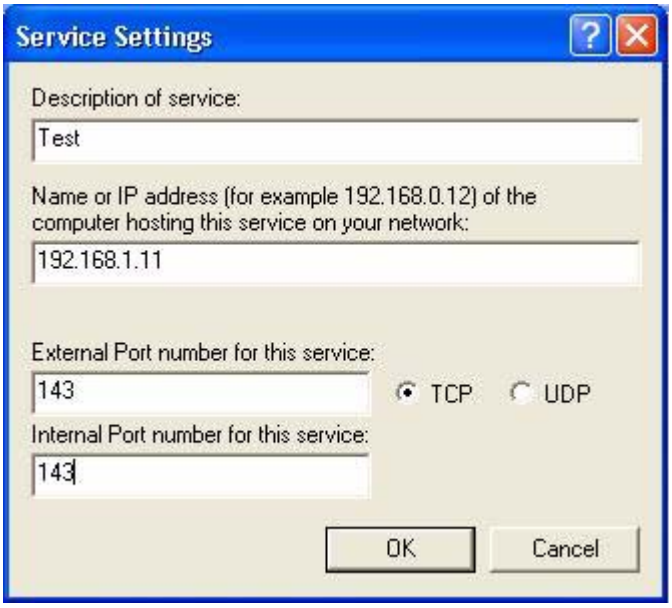
2 Right-click the icon and select **Properties**.

3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.





5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

7 Double-click on the icon to display your current Internet connection status.

Web Configurator Easy Access

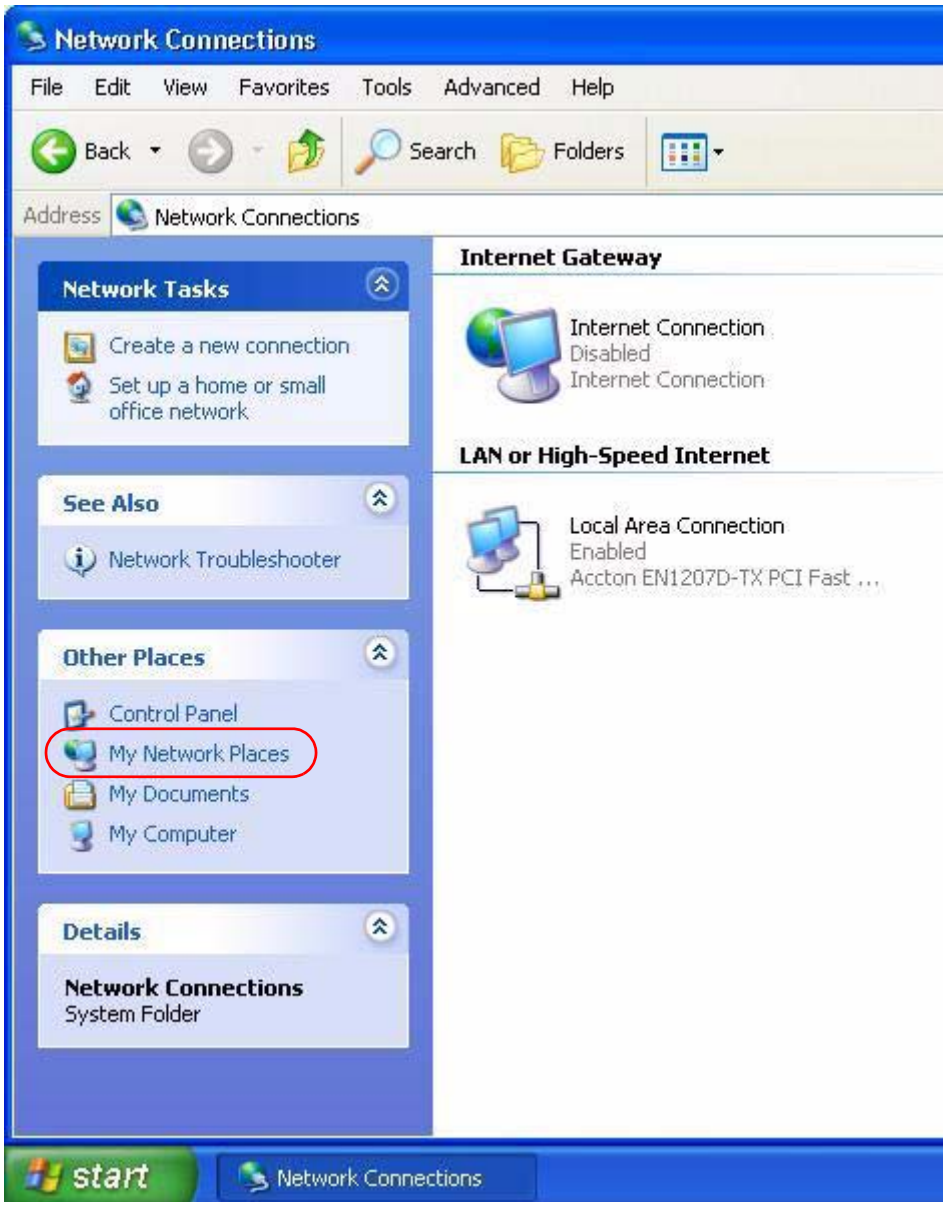
With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This comes helpful if you do not know the IP address of the ZyXEL Device.

Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.

6 Right-click on the icon for your ZyXEL Device and select **Properties**. A properties window displays with basic information about the ZyXEL Device.

PART V
Maintenance

System Settings (303)

Logs (309)

Update/Reboot (323)

Diagnostic (337)

Statistics (339)

20

System Settings

20.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

20.1.1 What You Can Do in the System Settings Screens

- Use the **General** screen (Section 20.2 on page 304) to configure system settings.
- Use the **Time Setting** screen (Section 20.3 on page 306) to set the system time.

20.1.2 What You Need to Know About System Settings

DHCP

DHCP (Dynamic Host Configuration Protocol) is a method of allocating IP addresses to devices on a network from a DHCP Server. Often your ISP or a router on your network performs this function.

LAN

A LAN (local area network) is typically a network which covers a small area, made up of computers and other devices which share resources such as Internet access, printers etc.

20.2 The General Screen

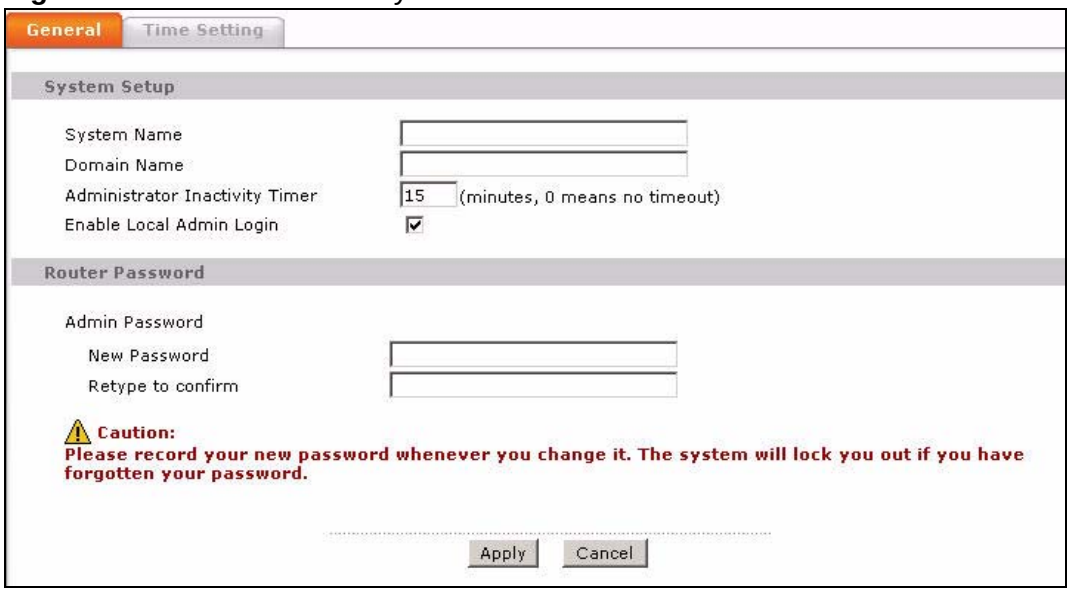
Use this screen to configure system settings such as the system and domain name, inactivity timeout interval and system password.

The **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name". Find the system name of your Windows computer by following one of the steps below.

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**.

Click **Maintenance > System** to open the **General** screen.

Figure 116 Maintenance > System > General



The following table describes the labels in this screen.

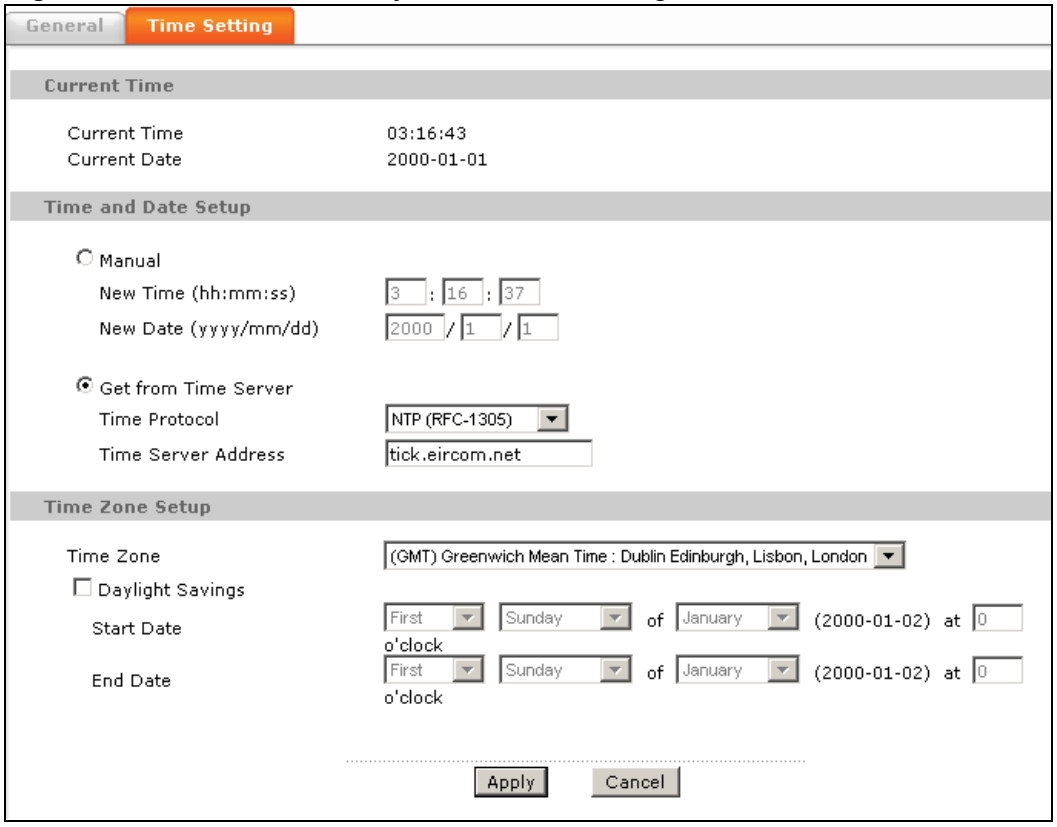
Table 86 Maintenance > System > General

LABEL	DESCRIPTION
System Setup	
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name. The **Domain Name** entry is propagated to the DHCP clients on the LAN.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or telnet) can be left idle before the session times out. The default is 15 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Enable Local Admin Login	By default, a password is required to login to the device. This by default is broadband1. A password can be disabled by deselecting the check box. Note: It is strongly recommended that you do not disable Local Admin Login and that you change the default login password.
Router Password	
Admin Password	
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Retype to confirm	Type the new password again for confirmation.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

20.3 The Time Setting Screen

Use this screen to configure the ZyXEL Device's time based on your local time zone. To change your ZyXEL Device's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown.

Figure 117 Maintenance > System > Time Setting



The following table describes the fields in this screen.

Table 87 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time	
Current Time	This field displays the time of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.
Current Date	This field displays the date of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.

Table 87 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the ZyXEL Device get the time and date from the time server you specified below.
Time Protocol	Select the time service protocol that your time server sends when you turn on the ZyXEL Device. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305)**, is similar to Time (RFC 868).
Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 87 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

21 Logs

21.1 Overview

This chapter contains information about configuring general log settings and viewing the ZyXEL Device's logs.

The web configurator allows you to choose which categories of events and/or alerts to have the ZyXEL Device log and then display the logs or have the ZyXEL Device send them to an administrator (as e-mail) or to a syslog server.

21.1.1 What You Can Do in the Log Screens

- Use the **View Log** screen (Section 21.2 on page 310) to see the logs for the categories that you selected in the **Log Settings** screen.
- Use The **Log Settings** screen (Section 21.3 on page 311) to configure the mail server, the syslog server, when to send logs and what logs to send.

21.1.2 What You Need To Know About Logs

Alerts

An alert is a message that is enabled as soon as the event occurs. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Logs

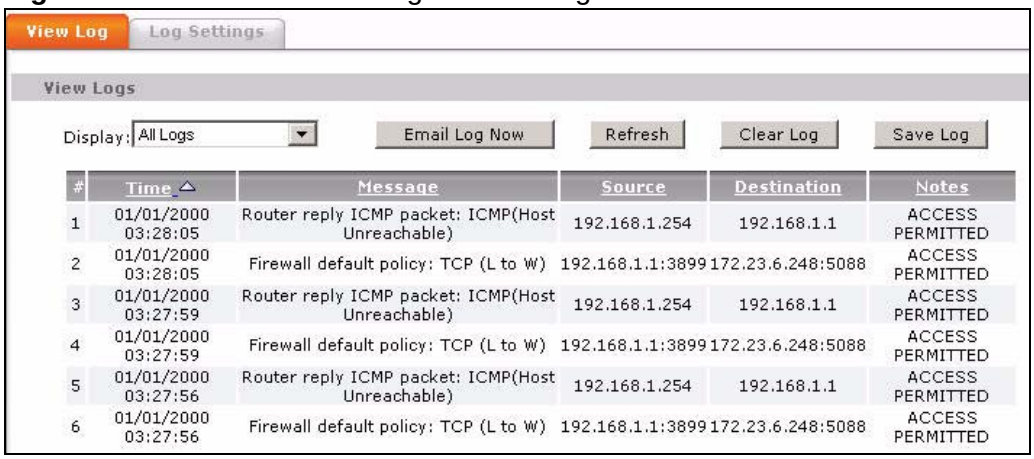
A log is a message about an event that occurred on your ZyXEL Device. For example, when someone logs in to the ZyXEL Device, you can set a schedule for how often logs should be enabled, or sent to a syslog server.

21.2 The View Log Screen

Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 21.3 on page 311). Click **Maintenance > Logs** to open the **View Log** screen.

Entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 118 Maintenance > Logs > View Log


View Log
Log Settings
View Logs
Display: All Logs
Email Log Now
Refresh
Clear Log
Save Log
Time Message Source Destination Notes
1 01/01/2000 03:28:05 Router reply ICMP packet: ICMP(Host Unreachable) 192.168.1.254 192.168.1.1 ACCESS PERMITTED
2 01/01/2000 03:28:05 Firewall default policy: TCP (L to W) 192.168.1.1:3899 172.23.6.248:5088 ACCESS PERMITTED
3 01/01/2000 03:27:59 Router reply ICMP packet: ICMP(Host Unreachable) 192.168.1.254 192.168.1.1 ACCESS PERMITTED
4 01/01/2000 03:27:59 Firewall default policy: TCP (L to W) 192.168.1.1:3899 172.23.6.248:5088 ACCESS PERMITTED
5 01/01/2000 03:27:56 Router reply ICMP packet: ICMP(Host Unreachable) 192.168.1.254 192.168.1.1 ACCESS PERMITTED
6 01/01/2000 03:27:56 Firewall default policy: TCP (L to W) 192.168.1.1:3899 172.23.6.248:5088 ACCESS PERMITTED

The following table describes the fields in this screen.

Table 88 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** screen display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Email Log Now	Click this to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **E-mail Log Settings** fields in **Log Settings**).
Refresh	Click this to renew the log screen.
Clear Log	Click this to delete all the logs.
Save Log	Click this to save the log record file to your computer.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.

Table 88 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.

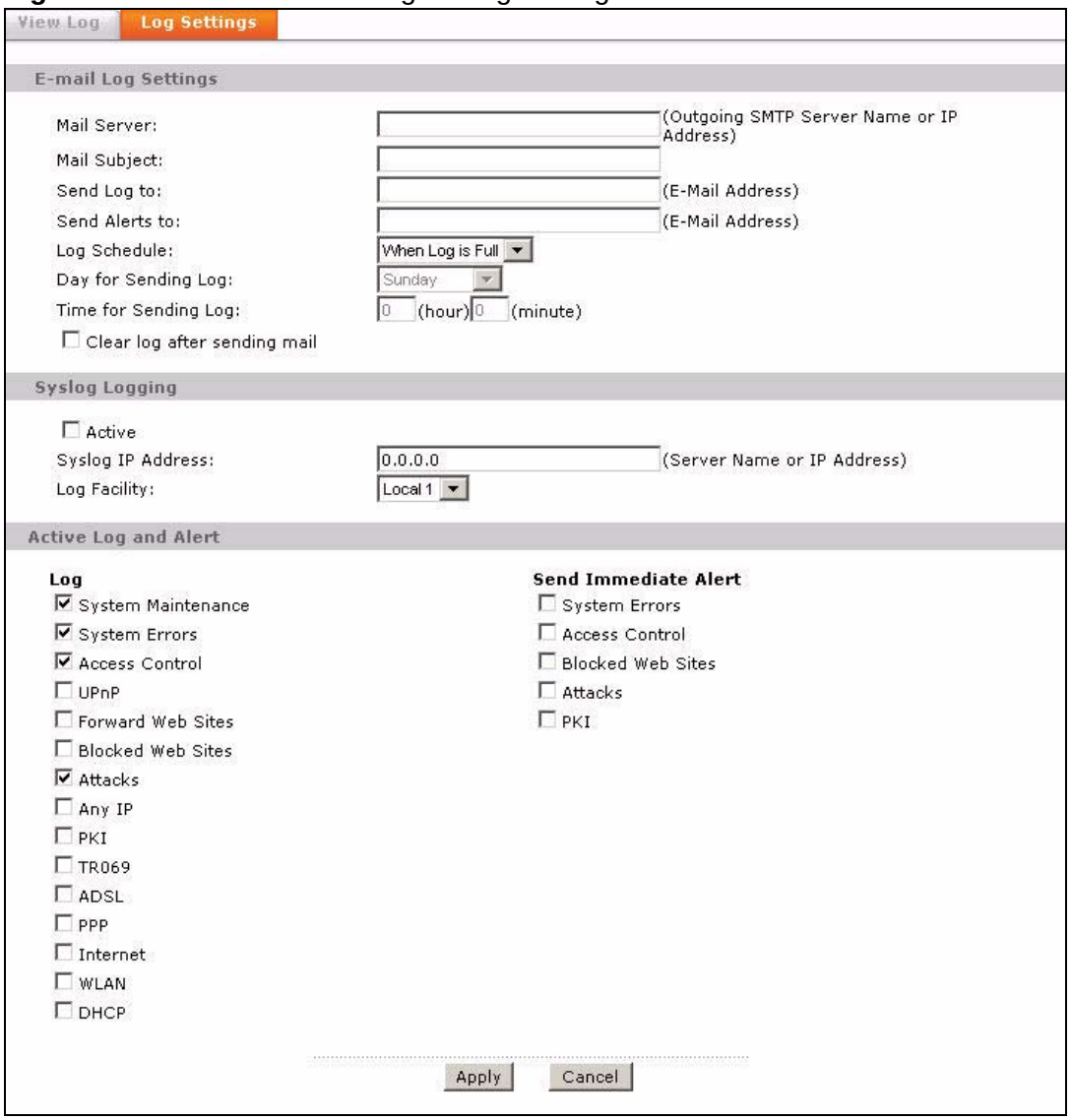
21.3 The Log Settings Screen

Use the **Log Settings** screen to configure the mail server, the syslog server, when to send logs and what logs to send.

To change your ZyXEL Device's log settings, click **Maintenance > Logs** > **Log Settings**. The screen appears as shown.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full. Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

Figure 119 Maintenance > Logs > Log Settings



The following table describes the fields in this screen.

Table 89 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends. Not all ZyXEL Device models have this field.

Table 89 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Send Log to	The ZyXEL Device sends logs to the e-mail address specified in this field. If this field is left blank, the ZyXEL Device does not send logs via e-mail.
Send Alerts to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • Daily • Weekly • Hourly • When Log is Full • None. If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the checkbox to delete all the logs after the ZyXEL Device sends an E-mail of the logs.
Syslog Logging	The ZyXEL Device sends a log to an external syslog server.
Active	Click **Active** to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record. Options include System Maintenance, System Errors, Access Control, UPnP, Forward Web Sites, Blocked Web Sites, Attacks, Any IP, PKI, TR069, ADSL, PPP, Internet, WLAN, and DHCP.
Send Immediate Alert	Select log categories for which you want the ZyXEL Device to send E-mail alerts immediately. Options include System Errors, Access Control, Blocked Web Sites, Attacks, and PKI.
Apply	Click this to save your customized settings and exit this screen.
Cancel	Click this to restore your previously saved settings.

21.4 SMTP Error Messages

If there are difficulties in sending e-mail the following error message appears.

“SMTP action request failed. ret= ??". The “??"are described in the following table.

Table 90 SMTP Error Messages

-1 means ZyXEL Device out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

21.4.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- "End of Log" message shows that a complete log has been sent.

Figure 120 E-mail Log Example

```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10 |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……..{snip}……..
……..{snip}……..
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |
End of Firewall Log
```

21.5 Log Descriptions

This section provides descriptions of example log messages.

Table 91 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
WAN interface gets IP: %s	A WAN interface got a new IP address from the DHCP, PPPoE, or dial-up server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
Successful WEB login	Someone has logged on to the router's web configurator interface.
WEB login failed	Someone has failed to log on to the router's web configurator interface.
Successful TELNET login	Someone has logged on to the router via telnet.
TELNET login failed	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the router via ftp.
FTP login failed	Someone has failed to log on to the router via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Starting Connectivity Monitor	Starting Connectivity Monitor.
Time initialized by Daytime Server	The router got the time and date from the Daytime server.
Time initialized by Time server	The router got the time and date from the time server.
Time initialized by NTP server	The router got the time and date from the NTP server.
Connect to Daytime server fail	The router was not able to connect to the Daytime server.
Connect to Time server fail	The router was not able to connect to the Time server.
Connect to NTP server fail	The router was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.
Configuration Change: PC = 0x%x, Task ID = 0x%x	The router is saving configuration changes.
Successful SSH login	Someone has logged on to the router’s SSH server.
SSH login failed	Someone has failed to log on to the router’s SSH server.

Table 91 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
Successful HTTPS login	Someone has logged on to the router's web configurator interface using HTTPS protocol.
HTTPS login failed	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.

Table 92 System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
setNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
readNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
WAN connection is down.	A WAN connection is down. You cannot access the network through this interface.

Table 93 Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]	The router blocked a packet that didn't have a corresponding NAT table entry.
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.

Table 94 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen.
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
Firewall session time out, sent TCP RST	The router sent a TCP reset packet when a dynamic firewall session timed out.Default timeout values:ICMP idle timeout (s): 60UDP idle timeout (s): 60TCP connection (three way handshaking) timeout (s): 30TCP FIN-wait timeout (s): 60TCP idle (established) timeout (s): 3600
Exceed MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > “Maximum Incomplete High”, the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < “Maximum Incomplete Low”.
Access block, sent TCP RST	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: "sys firewall tcprst").

Table 95 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
[TCP | UDP | ICMP | IGMP | Generic] packet filter matched (set: %d, rule: %d)	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

For type and code details, see Table 104 on page 321.

Table 96 ICMP Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: ICMP	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: ICMP	The router blocked a packet that didn't have a corresponding NAT table entry.
Unsupported/out-of-order ICMP: ICMP	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
Router reply ICMP packet: ICMP	The router sent an ICMP reply packet to the sender.

Table 97 CDR Logs

LOG MESSAGE	DESCRIPTION
board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or "ch" is the call channel ID.For example,"board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.
board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s	The PPPoE, PPTP or dial-up call is connected.
board %d line %d channel %d, call %d, %s C02 Call Terminated	The PPPoE, PPTP or dial-up call was disconnected.

Table 98 PPP Logs

LOG MESSAGE	DESCRIPTION
ppp:LCP Starting	The PPP connection's Link Control Protocol stage has started.
ppp:LCP Opening	The PPP connection's Link Control Protocol stage is opening.
ppp:CHAP Opening	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
ppp:IPCP Starting	The PPP connection's Internet Protocol Control Protocol stage is starting.
ppp:IPCP Opening	The PPP connection's Internet Protocol Control Protocol stage is opening.

Table 98 PPP Logs (continued)

LOG MESSAGE	DESCRIPTION
ppp:LCP Closing	The PPP connection's Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection's Internet Protocol Control Protocol stage is closing.

Table 99 UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 100 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: block keyword	The content of a requested web page matched a user defined keyword.
%s	The system forwarded web content.

For type and code details, see Table 104 on page 321.

Table 101 Attack Logs

LOG MESSAGE	DESCRIPTION
attack [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack.
land [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack.
ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack.
illegal command TCP	The firewall detected a TCP illegal command attack.

Table 101 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.

Table 102 802.1X Logs

LOG MESSAGE	DESCRIPTION
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.
User logout because of user request.	A user logged out.
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.
No Server to authenticate user.	There is no authentication server to authenticate a user.

Table 103 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.

Table 103 ACL Setting Notes (continued)

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to L/ZyXEL Device)	LAN to LAN/ ZyXEL Device	ACL set for packets traveling from the LAN to the LAN or the ZyXEL Device.
(W to W/ZyXEL Device)	WAN to WAN/ ZyXEL Device	ACL set for packets traveling from the WAN to the WAN or the ZyXEL Device.

Table 104 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request

Table 104 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	Information request message
16		Information Reply
	0	Information reply message

Table 105 Syslog Logs

LOG MESSAGE	DESCRIPTION
<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>	"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU->LOGS->Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to RFC 2408 for detailed information on each type.

Table 106 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

22

Update/Reboot

22.1 Overview

This chapter explains how to upload new firmware, manage configuration files and restart your ZyXEL Device.

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

Only use firmware for your device's specific model. Refer to the label on the bottom of your ZyXEL Device.

22.1.1 What You Can Do in the Update/Reboot Screens

- Use the **Firmware Upgrade** screen (Section 22.2 on page 331) to upload firmware to your device.
- Use the **Configuration** screen (Section 22.3 on page 333) to backup and restore device configurations. You can also reset your device settings back to the factory default.
- Use the **Restart** screen (Section 22.4 on page 336) to restart your ZyXEL device.

22.1.2 What You Need To Know About Update/Reboot

Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a “rom” filename extension. Once you have customized the ZyXEL Device's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. Find this firmware at www.zyxel.com.With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the ZyXEL Device.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file “config.cfg”.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyXEL Device only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyXEL Device and the external filename refers to the filename not on the ZyXEL Device, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **Status** screen to confirm that you have uploaded the correct firmware version.

Table 107 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the ZyXEL Device. Uploading the rom-0 file replaces the entire ROM file system, including your ZyXEL Device configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the ZyXEL Device.	*.bin

FTP Restrictions

FTP will not work when:

1. The firewall is active (turn the firewall off or create a firewall rule to allow access from the WAN).
2. You have disabled the FTP service in the **Remote Management** screen.
3. The IP you entered in the Secured Client IP field does not match the client IP. If it does not match, the device will disallow the FTP session.

22.1.3 Before You Begin

- Ensure you have either created a firewall rule to allow access from the WAN or turned the firewall off, otherwise the FTP will not function.
- FTP service is disabled by default. Make sure to activate the FTP service in the Remote Management screen.

22.1.4 Tool Examples

Using FTP or TFTP to Restore Configuration

This example shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device. When the Restore Configuration process is complete, the device automatically restarts.

Restore Using FTP Session Example

Figure 121 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to Section 22.1.2 on page 324 to read about configurations that disallow TFTP and FTP over WAN.

FTP and TFTP Firmware and Configuration File Uploads

These examples show you how to upload firmware and configuration files.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device.

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client. The following sections give examples of how to upload the firmware and the configuration files.

FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your device.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “broadband1”).
5. Enter “bin” to set transfer mode to binary.
6. Use “put” to transfer files from the computer to the device, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the device and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the ftp prompt.

FTP Session Example of Firmware File Upload

Figure 122 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed in this chapter.

Refer to Section 22.1.2 on page 324 to read about configurations that disallow TFTP and FTP over WAN.

TFTP File Upload

The device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the device and log in. Because TFTP does not have any security checks, the device records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Enter the command “sys stdio 0” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute management idle timeout (default) when the file transfer is complete.
3. Launch the TFTP client on your computer and connect to the device. Set the transfer mode to binary before starting data transfer.
4. Use the TFTP client (see the example below) to transfer files between the device and the computer. The file name for the firmware is “ras”.

   Note that the telnet connection must be active and the device in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For

UNIX, use “get” to transfer from the device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the device’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the device).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

Using the FTP Commands to Back Up Configuration

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your ZyXEL Device.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “broadband1”).
5. Enter “bin” to set transfer mode to binary.
6. Use “get” to transfer files from the ZyXEL Device to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyXEL Device to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the ftp prompt.

FTP Command Configuration Backup Example

This figure gives an example of using FTP commands from the DOS command prompt to save your device's configuration onto your computer.

Figure 123 FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Configuration Backup Using GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 108 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

Backup Configuration Using TFTP

The ZyXEL Device supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1 Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.

2 Enter command "sys stdio 0" to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter command "sys stdio 5" to restore the five-minute management idle timeout (default) when the file transfer is complete.

3 Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.

4 Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the configuration file is "rom-0" (rom-zero, not capital o).

Note that the telnet connection must be active before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the ZyXEL Device to the computer and "binary" to set binary transfer mode.

TFTP Command Configuration Backup Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the ZyXEL Device IP address, "get" transfers the file source on the ZyXEL Device (rom-0, name of the configuration file on the ZyXEL Device) to the file destination on the computer and renames it config.rom.

Configuration Backup Using GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 109 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyXEL Device. 192.168.1.1 is the ZyXEL Device's default IP address when shipped.
Send/ Fetch	Use "Send" to upload the file to the ZyXEL Device and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyXEL Device. The filename for the firmware is "ras" and for the configuration file, is "rom-0".

Table 109 General Commands for GUI-based TFTP Clients (continued)

COMMAND	DESCRIPTION
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

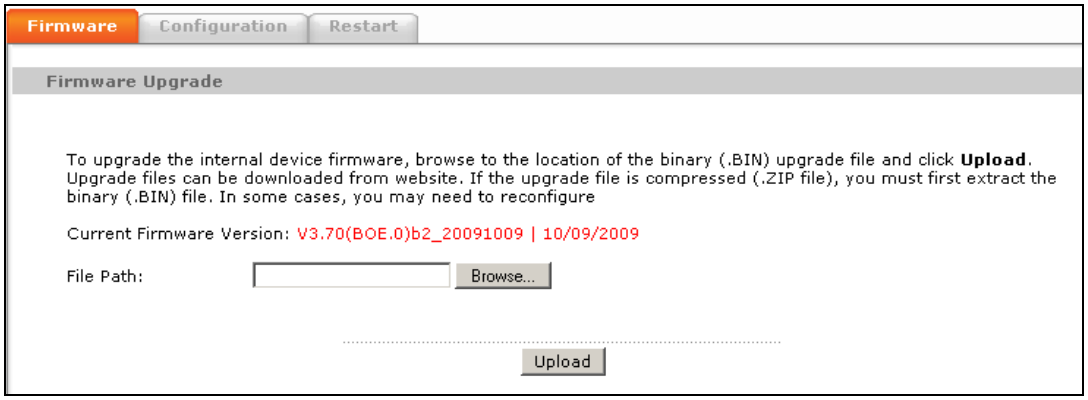
Refer to Section 22.1.2 on page 324 to read about configurations that disallow TFTP and FTP over WAN.

22.2 The Firmware Screen

Click **Maintenance > Update / Reboot** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to 3 minutes. After a successful upload, the system will reboot. See Section 22.1.4 on page 325 for upgrading firmware using FTP/TFTP commands.

Do NOT turn off the ZyXEL Device while firmware upload is in progress!

Figure 124 Maintenance > Update/Reboot > Firmware


Firmware
Configuration
Restart
Firmware Upgrade
To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure
Current Firmware Version: V3.70(BOE.0)b2_20091009 | 10/09/2009
File Path:
Browse...
Upload

The following table describes the labels in this screen.

Table 110 Maintenance > Tools > Firmware

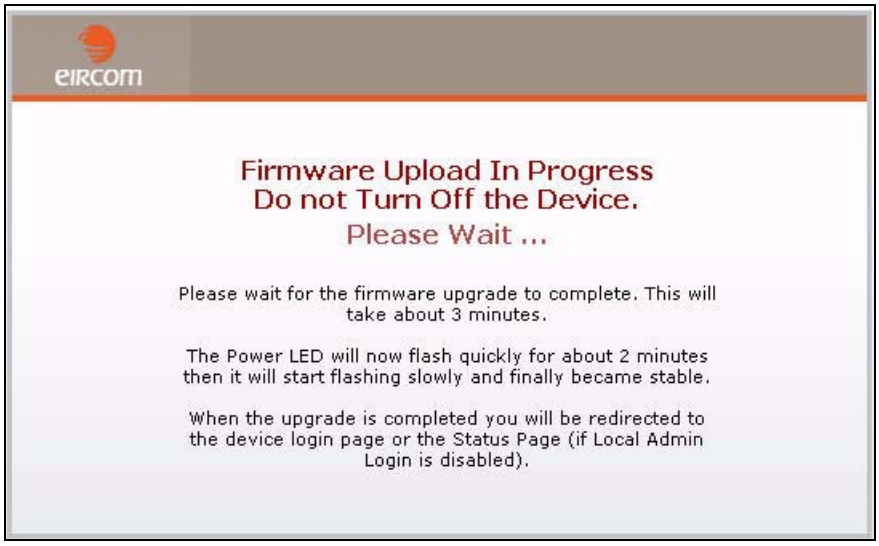
LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.

Table 110 Maintenance > Tools > Firmware (continued)

LABEL	DESCRIPTION
Browse...	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Progress** screen, wait 3 minutes before logging into the ZyXEL Device again.

Figure 125 Firmware Upload In Progress


eircom
Firmware Upload In Progress
Do not Turn Off the Device.
Please Wait ...
Please wait for the firmware upgrade to complete. This will take about 3 minutes.
The Power LED will now flash quickly for about 2 minutes then it will start flashing slowly and finally became stable.
When the upgrade is completed you will be redirected to the device login page or the Status Page (if Local Admin Login is disabled).

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 126 Network Temporarily Disconnected

After three minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

Figure 127 Error Message

System Upload
Firmware upload error!
The uploaded file was not accepted by the device. Please return to the previous page and select a valid upgrade file.
Click Help for more information.
Return

22.3 The Configuration Screen

See Section 22.1.4 on page 325 for transferring configuration files using FTP/TFTP commands.

Click **Maintenance > Update / Reboot > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 128 Maintenance > Update/Reboot > Configuration

Firmware
Configuration
Restart
Backup Configuration
Click Backup to save the current configuration to you computer.
Backup
Restore Configuration
To restore a previously saved configuration file please click Browse to locate one, and then click Upload.
File Path:
Browse...
Upload
Reset to Factory Default Settings
Click Reset to clear all user-entered configurations and return the device to its factory default settings.
The following default settings would become effective after click Reset
Password : broadband1
Lan IP : 192.168.1.254
DHCP : Server .
Reset

Backup Configuration

Backup Configuration allows you to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your

configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyXEL Device's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

Table 111 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.

Do not turn off the ZyXEL Device while configuration file upload is in progress.

After you see a "restore configuration successful" screen, you must then wait 1 minute before logging into the ZyXEL Device again.

Figure 129 Configuration Upload Successful

eircom
Restore Configuration successful
The Router Is Rebooting Now.
Please Wait ...
This process will take about 1 minute.
When the reboot is completed, you will be redirected to
the device login page or the Status Page (if Local Admin
Login is disabled).

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 130 Network Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.254). See Appendix A on page 361 for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

Figure 131 Configuration Upload Error

System Restore
Restore configuration error!
The configuration file was not accepted by the device. Please return to the previous page and select a valid configuration file. Click Help for more information.
Return

Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. The following warning screen appears.

Figure 132 Reset Warning Message

Microsoft Internet Explorer
Are you sure you want to reset the device back to the factory defaults?This will erase all of your custom configuration.
OK
Cancel

Figure 133 Reset In Process Message

eircom
Reset to Factory Default Settings
Please Wait ...
The device will now reboot.
This process will take about 1 minute.
When the factory reset is complete, you will be redirected to the device login page.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device. Refer to Section 1.6 on page 27 for more information on using the **RESET** button.

22.4 The Restart Screen

System restart allows you to reboot the ZyXEL Device remotely without turning the power off. You may need to do this if the ZyXEL Device hangs, for example.

Click **Maintenance > Update/Reboot** > **Restart**. Click **Restart** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

Figure 134 Maintenance > Update/Reboot >Restart

Firmware
Configuration
Restart
System Reboot
Click Restart for the device to perform a software reboot. This will take about 1 minute. When the device reboots the Power LED will flash and then become steady if the reboot is successful. After the reboot you will be redirected to the device login page or the device Status Page (if Local Admin Login is disabled).
Restart

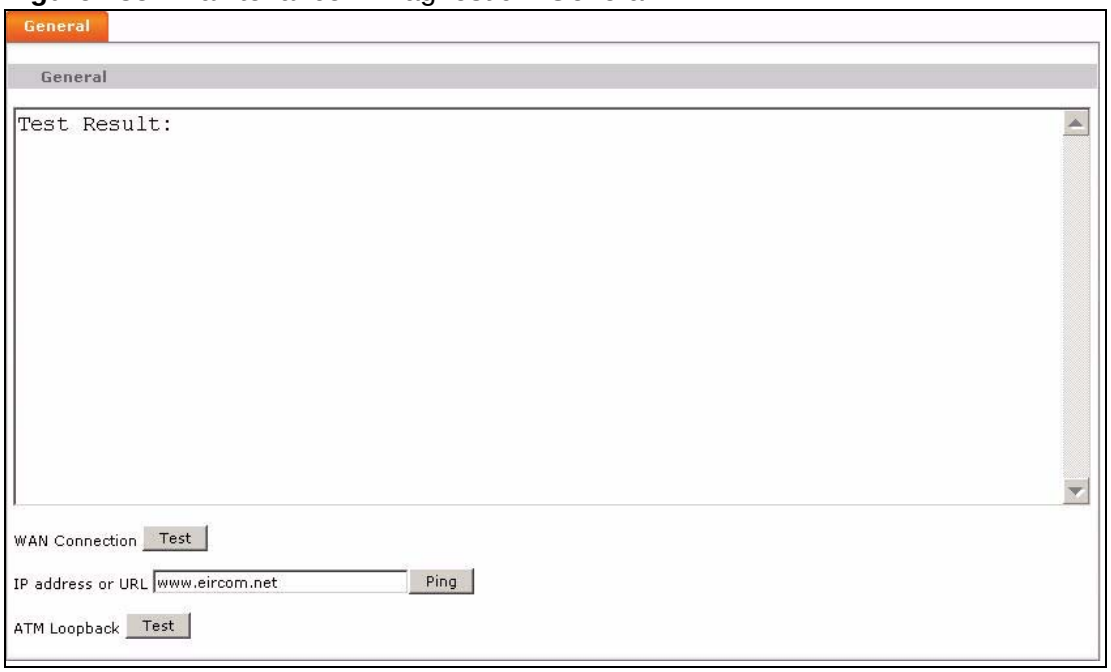
23

Diagnostic

23.1 The Diagnostic General Screen

Use this screen to test your WAN connection, ping an IP address, or test ATM loopback. Click **Maintenance > Diagnostic** to open the screen shown next.

Figure 135 Maintenance > Diagnostic > General



The following table describes the fields in this screen.

Table 112 Maintenance > Diagnostic > General

LABEL	DESCRIPTION
WAN Connection Test	Click this to check your WAN connection status of DSL, ATM, Ethernet PPPoE, IP, and Pinging.
IP Address or URL	Type the IP address or URL of a computer that you want to ping in order to test a connection.

Table 112 Maintenance > Diagnostic > General

LABEL	DESCRIPTION
Ping	Click this to ping the IP address that you entered.
ATM Loopback Test	Click this to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The ZyXEL Device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the ZyXEL Device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.

24

Statistics

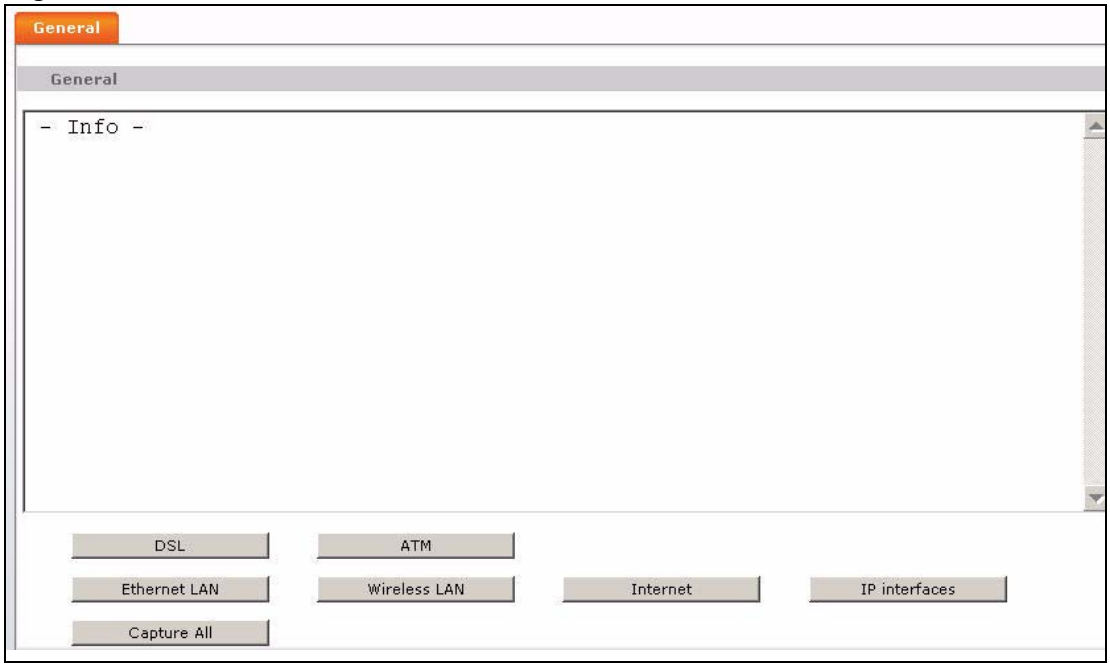
24.1 The Statistics General Screen

You can view the DSL and Ethernet WAN connection statistics in the Statistics screen. The statistics displayed can help you identify connection problems. Errors are common in all network connections. Too many errors may indicate a problem. These statistics help experienced networking professionals identify the problem and hopefully fix it. Excess errors may occur if there is a lot of traffic on your network. Reducing usage of the network will decrease errors displayed here.

If you need to contact your vendor or customer support, you may be asked to copy and send data from the Statistics screen. See the Network Connections section in Troubleshooting if you are experiencing problems with your Internet connection.

Click **Maintenance > Statistics** to open the screen shown next.

Figure 136 Maintenance > Statisticsl



The following table describes the fields in this screen.

LABEL	DESCRIPTION
DSL	Click this to view statistics about the DSL connections.
ATM	Click this to view your DSL connection's Asynchronous Transfer Mode (ATM) statistics. ATM is a networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. The (Segmentation and Reassembly) SAR driver translates packets into ATM cells. It also receives ATM cells and reassembles them into packets. These counters are set back to zero whenever the device starts up.
Ethernet LAN	Click this to view statistics about the Ethernet LAN.
Wireless LAN	Click this to view statistics about the Wireless LAN.
Internet	Click this to view statistics about the Internet.
IP Interfaces	Click this to view statistics about the IP Interfaces.
Capture All	Click this to display information and statistics about your ZyXEL Device's DSL connection, ATM, Ethernet LAN, Wirelss LAN, Inernet and IP Interfaces.

24.1.1 Terms

Here is a brief overview of what some of the terms displayed in the Statistics screen mean.

Your modem or router is the near end and the device at your broadband service provider, the DSLAM (Digital Subscriber Line Access Multiplexer), is the far end. A near end error is one that happened in the data traveling from the DSLAM to your modem or router. A far end error is one that happened in the data traveling from your modem or router to the DSLAM.

Fast and interleaving are methods of transferring data. Fast sends data in contiguous packets. Interleaving rearranges packets and reassembles them again on the other side.

Noise on a line can cause data to become corrupt so your modem or router has to request all (if using fast) or some (if using interleaving) to be sent again. This slows down the overall data transmission rate.

Interleaving is better on telephone lines with more than average noise or where the DSL service provider is not near your residence as your modem or router will be able to either re-assemble the data or just request the part of the data that it is unable to recover to be sent again.

The method your modem or router use depends on what the DSLAM is using.

When data packets are transmitted they contain control bits that enable your modem or router to check and correct a certain amount of erroneous bits. This type of error checking is known as Forward Error Correction (FEC). FEC errors are correctable.

Noise margin downstream is the signal to noise ratio for the downstream part of the connection (coming into the ZyXEL Device from the ISP). It is measured in decibels. The higher the number the more signal and less noise there is.

Output power upstream is the amount of power (in decibels) that the ZyXEL Device is using to transmit to the ISP.

Attenuation downstream is the reduction in amplitude (in decibels) of the DSL signal coming into the ZyXEL Device from the ISP.

Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each called tones. The rest of the display is the line's bit allocation. This is displayed as the number (in hexadecimal format) of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support certain ADSL transmission rates, and possibly to determine whether particular specific types of interference or line attenuation exist. Refer to the ITU-T G.992.1 recommendation for more information on DMT.

The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15. There will be some tones without any bits as there has to be space between the upstream and downstream channels.

A **Cyclic Redundancy Check (CRC)** is an error detecting code that discovers errors that cannot be corrected. Data packets containing CRC errors need to be re-sent.

Header Error Correction (HEC) errors are similar to CRC errors, except only the header of the ATM cell is checked.

Typically one type of error causes others too, and as mentioned, some errors are normal on a DSL line.

PART VI
Troubleshooting and Specifications

Troubleshooting (345)

Product Specifications (351)

25

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyXEL Device Access and Login
- Internet Access
- Network Connections

25.1 Power, Hardware Connections, and LEDs

The ZyXEL Device does not turn on. None of the LEDs turn on.

1. Make sure the ZyXEL Device is turned on.
2. Make sure you are using the power adaptor or cord included with the ZyXEL Device.
3. Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the ZyXEL Device off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 26.

2 Check the hardware connections.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Turn the ZyXEL Device off and on.

5 If the problem continues, contact the vendor.

25.2 ZyXEL Device Access and Login

I forgot the IP address for the ZyXEL Device.

1 The default IP address is **192.168.1.254**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 27.

I forgot the password.

1 The default admin password is **broadband1**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 27.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.254.

- If you changed the IP address (Section 6.2 on page 113), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyXEL Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.5 on page 26 for more information on LED status.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix B on page 385.

4 If you disabled **Any IP** (Section 6.6.7 on page 125), make sure your computer is in the same subnet as the ZyXEL Device. (If you know that there are routers between your computer and the ZyXEL Device, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Appendix A on page 361. Your ZyXEL Device is a DHCP server by default.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the ZyXEL Device. See Appendix A on page 361.

5 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See Section 1.6 on page 27.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings and firewall rules to find out why the ZyXEL Device does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the ZyXEL Device.

1 Make sure you have entered the password correctly. The default admin password is **broadband1**. The field is case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.

3 Turn the ZyXEL Device off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 25.1 on page 345.

I cannot Telnet to the ZyXEL Device.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

FTP service is disabled by default. Make sure to activate the FTP service in the Remote Management screen.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

25.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.5 on page 26 for more information on LED status.

2 Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.

4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.5 on page 26 for more information on LED status.

2 Turn the ZyXEL Device off and on.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 26. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

1 Check the signal strength. If the signal strength is low, try moving your computer closer to the ZyXEL Device if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

2 Turn the ZyXEL Device off and on.

3 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

25.4 Network Connections

My network cannot be connected. How can I check the Internet connection status?

1 Check the LEDs on the ZyXEL Device for the following situations:

- If the DSL LED is off, there is no DSL connection. Check if your cables are connected properly to the ZyXEL Device.
- If the DSL LED is blinking green, the ZyXEL Device is initializing the DSL line. If it keeps blinking for a long time, please reboot the device.
- If the DSL LED lights green and the Internet LED lights red, the ZyXEL Device has failed to get an IP address from your broadband service supplier. Please contact your vendor or customer support.
- If the DSL LED lights green but the Internet LED is off, the ZyXEL Device does not have an IP connection. Please check if you have entered the correct ISP account and password when setting up the Internet connection. If the status is the same, reboot the device. If the problem remains, please contact your vendor or customer support.

2 Excess errors may occur if the quality of your line is poor. If you hear noise on the line while making a telephone call, you should ask your local telecommunications office to check the lines in your house or apartment building and the line from your residence to your DSL service provider.

26

Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

26.1 Hardware Specifications

Table 113 Hardware Specifications

Dimensions	191 x 154 x 32mm
Weight	290g
Power Specification	12VDC 1A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
ADSL Port	1 RJ-11 FXS POTS port
RESET Button	Restores factory defaults
Antenna	One fixed external antenna, 5dBi
WPS WIFI Button	5 ~ 6 seconds: turn on or off WLAN (WLAN on by default) 1 ~ 2 seconds: enable WPS (Wi-Fi Protected Setup)
Operation Temperature	0º C ~ 40º C
Storage Temperature	-20º ~ 60º C
Operation Humidity	20% ~ 90% RH
Storage Humidity	20% ~ 90% RH

26.2 Firmware Specifications

Table 114 Firmware Specifications

Default IP Address	192.168.1.254
Default Subnet Mask	255.255.255.0 (24 bits)

Table 114 Firmware Specifications (continued)

Default Admin Password	broadband1
DHCP Server IP Pool	192.168.1.1 to 192.168.1.200
Static DHCP Addresses	10
Content Filtering	Web page blocking by URL keyword.
Static Routes	16
Device Management	Use the web configurator to easily configure the rich range of features on the ZyXEL Device.
Wireless Functionality (wireless devices only)	Allow the IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the ZyXEL Device wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration. You can put it back on the ZyXEL Device later if you decide to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logs	Use logs for troubleshooting. You can send logs from the ZyXEL Device to an external syslog server.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

Table 114 Firmware Specifications (continued)

Firewall	Your device has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.
Content Filtering	Content filtering allows you to block access to Internet web sites that contain key words (that you specify) in the URL. You can also schedule when to perform the filtering and give trusted LAN IP addresses unfiltered Internet access.
QoS (Quality of Service)	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyXEL Device.
Any IP	The Any IP feature allows a computer to access the Internet and the ZyXEL Device without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.
PPPoE Support (RFC2516)	PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.
Other PPPoE Features	PPPoE idle time out PPPoE dial on demand
Multiple PVC (Permanent Virtual Circuits) Support	Your device supports up to 8 Permanent Virtual Circuits (PVCs).
IP Alias	IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network.
Packet Filters	Your device's packet filtering function allows added network security and management.
WAN IP Passthrough	This allows a WAN computer on the local network of the ZyXEL Device to have access to web services using the public IP address. When WAN IP Passthrough is configured, all traffic is forwarded to the computer and will not go through NAT.
VLANs	This allows a physical network to be partitioned into multiple logical networks.

Table 114 Firmware Specifications (continued)

ADSL Standards	ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2). EOC specified in ITU-T G.992.1 ADSL2 G.dmt.bis (G.992.3) ADSL2 G.lite.bis (G.992.4) ADSL2+ (G.992.5) Extended-Reach ADSL (ER ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC2684/1483) PPP over ATM AAL5 (RFC2364) PPP over Ethernet for DSL connection (RFC2516) VC-based and LLC-based multiplexing Support up to 8 PVCs I.610 F4/F5 OAM TR-067/TR-100

Table 114 Firmware Specifications (continued)

Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol IP routing Transparent bridging for unsupported network layer protocols RIP I/RIP II ICMP ATM QoS IP Multicasting IGMP v1 and v2 IGMP Proxy 802.1Q/1P
Management	Embedded Web Configurator CLI (Command Line Interpreter) Embedded FTP/TFTP Server for firmware upgrade and configuration file backup and restore Telnet for remote management Remote Management Control: WWW, Telnet, FTP, DNS, and ICMP. Remote Firmware Upgrade Syslog TR-069 F4/F5 OAM

26.3 Wireless Features

Table 115 Wireless Features

External Antenna	The ZyXEL Device is equipped with one fixed antenna to provide a clear radio signal between the wireless stations and the access points.
Wireless LAN MAC Address Filtering	Your device can check the MAC addresses of wireless stations against a list of allowed or denied MAC addresses.
WEP Encryption	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.
Wi-Fi Protected Access	Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security standard. Key differences between WPA and WEP are user authentication and improved data encryption.
WPA2	WPA 2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Table 115 Wireless Features

WMM QoS	WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic according to the delivery requirements of individual services.
Other Wireless Features	IEEE 802.11b/g Compliance Frequency Range: 2.4 GHz ISM Band WDS (wireless client: G-570S v2) Auto channel selection Advanced Orthogonal Frequency Division Multiplexing (OFDM) Data Rates: 54Mbps and Auto Fallback WPA, WPA-PSK WPA2, WPA2-PSK WMM QoS Wired Equivalent Privacy (WEP) Data Encryption 64/128/256 bit. WLAN bridge to LAN Up to 32 MAC Address filters IEEE 802.1x External RADIUS server using EAP-MD5, TLS, TTLS Wireless scheduling Wireless output power adjustment Configurable remote access for WLAN WIFI button

The following list, which is not exhaustive, illustrates the standards supported in the ZyXEL Device.

Table 116 Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol.
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 2236	Internet Group Management Protocol, Version 2.

Table 116 Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 2364	PPP over AAL5 (PPP over ATM over ADSL)
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5.
RFC 2766	Network Address Translation - Protocol
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/ WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g+	Turbo and Super G modes
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
ANSI T1.413, Issue 2	Asymmetric Digital Subscriber Line (ADSL) standard.
G dmt(G.992.1)	G.992.1 Asymmetrical Digital Subscriber Line (ADSL) Transceivers
ITU G.992.1 (G.DMT)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.2 (G. Lite)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.3 (G.dmt.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.4 (G.lite.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.5 (ADSL2+)	ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits.
Microsoft PPTP	MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)
RFC 2383	ST2+ over ATM Protocol Specification - UNI 3.1 Version
TR-069	TR-069 DSL Forum Standard for CPE Wan Management.
1.363.5	Compliant AAL5 SAR (Segmentation And Re-assembly)

26.4 Power Adaptor Specifications

Table 117 ZyXEL Device Series Power Adaptor Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	12V 1A SOCB PA
Input Power	AC 120Volts/60Hz
Output Power	DC 12Volts/1.0A
Power Consumption	7.7 Watt max
Safety Standards	ANSI/UL 60950-1, CSA 60950-1
EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	
Input Power	AC 230Volts/50Hz
Output Power	DC 12Volts/1.0A
Power Consumption	8 Watt max
Safety Standards	CE, GS or TUV, EN60950-1

PART VII Appendices and Index

Note: The appendices provide general information. Some details may not apply to your ZyXEL Device.

Setting up Your Computer's IP Address (361)

Pop-up Windows, JavaScripts and Java Permissions (385)

IP Addresses and Subnetting (395)

Wireless LANs (405)

Services (421)

Legal Information (425)

Index (429)

A

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP/Vista, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

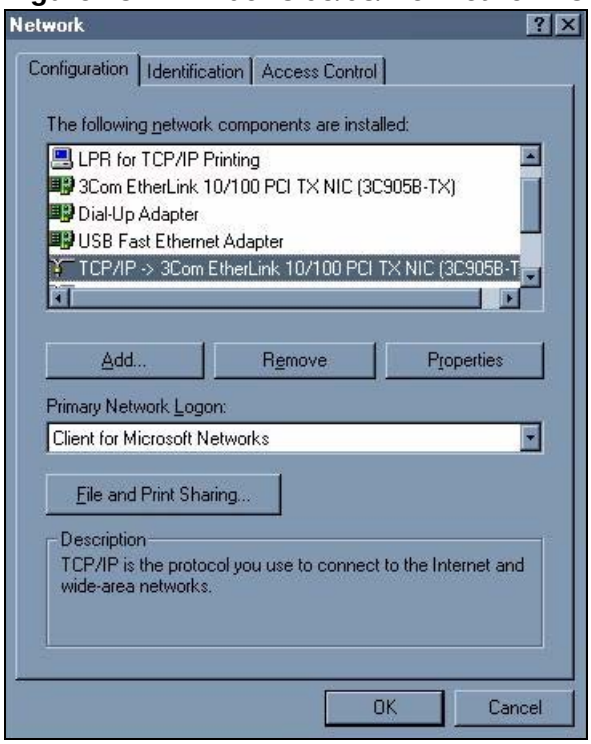
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyXEL Device's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 137 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.

3 Select **Microsoft** from the list of **manufacturers**.

4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.

2 Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

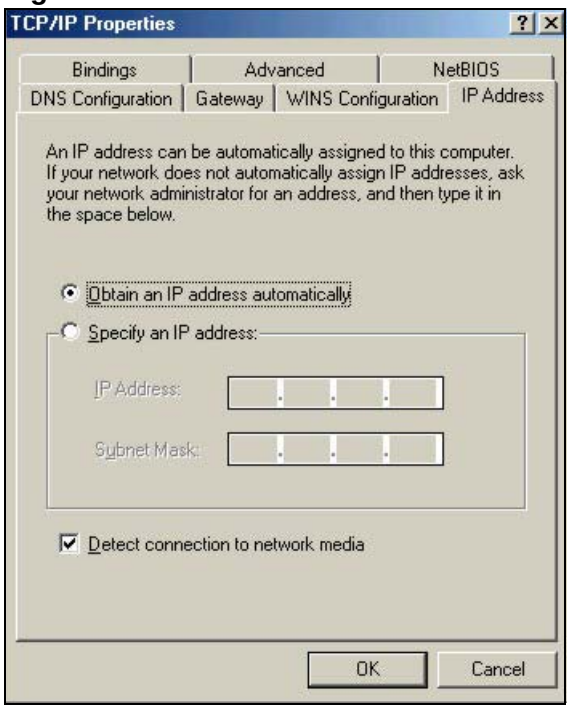
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

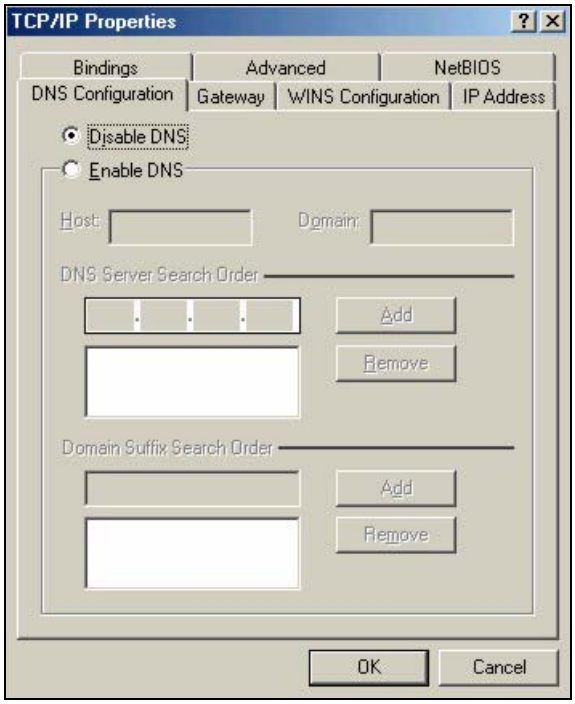
Figure 138 Windows 95/98/Me: TCP/IP Properties: IP Address


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 139 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your ZyXEL Device and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

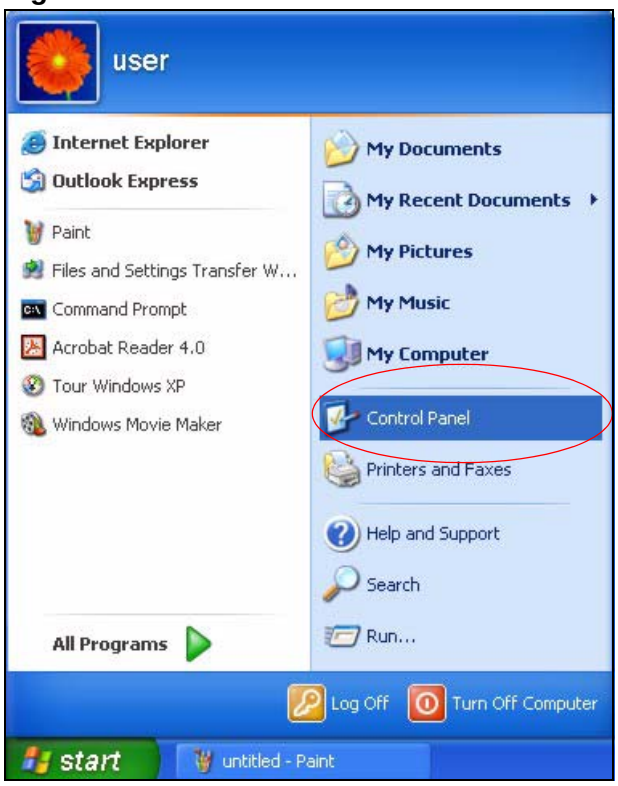
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 140 Windows XP: Start Menu



2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

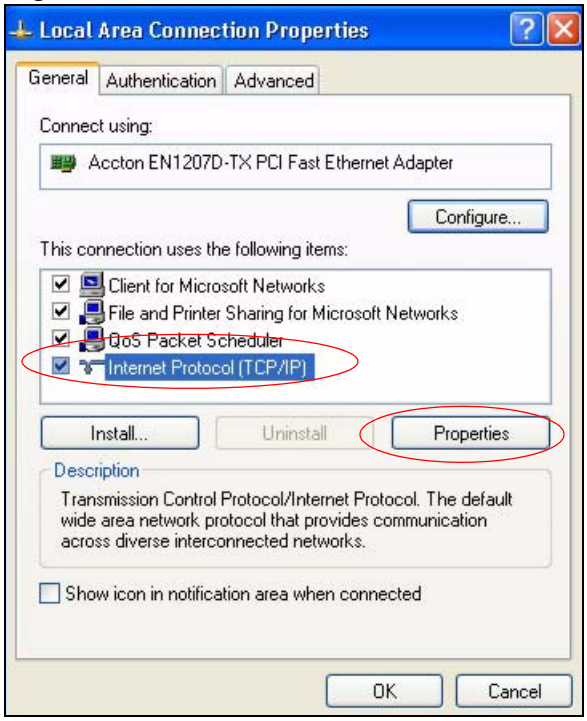
Figure 141 Windows XP: Control Panel

3 Right-click **Local Area Connection** and then click **Properties**.

Figure 142 Windows XP: Control Panel: Network Connections: Properties

4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

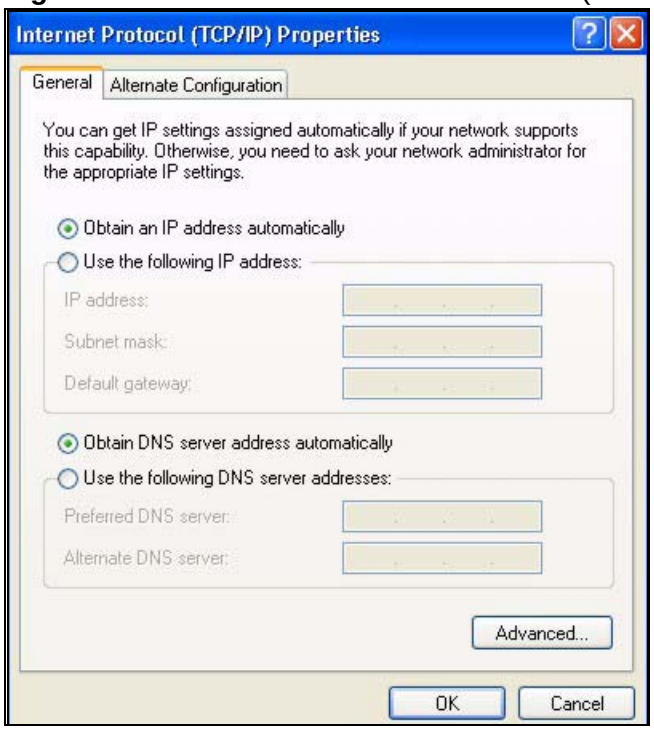
Figure 143 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 144 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

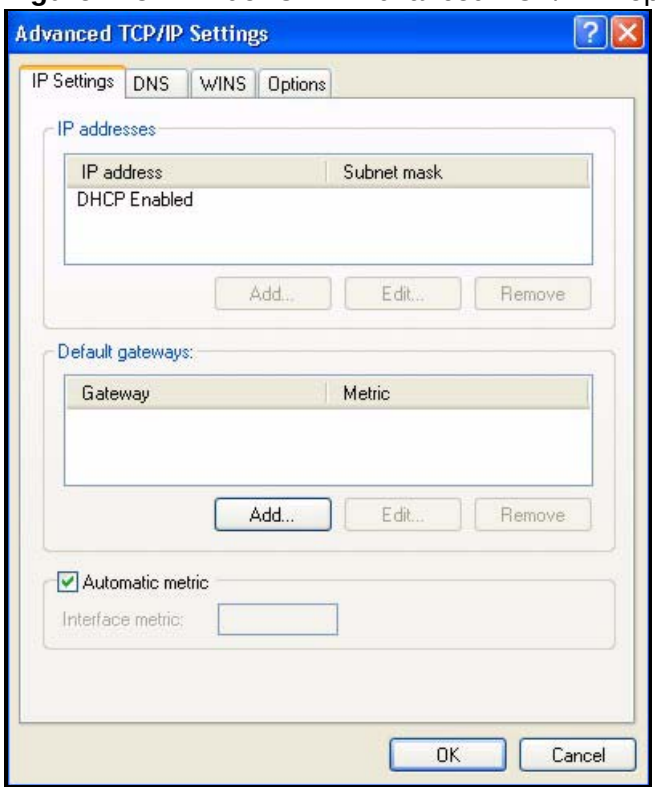
6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

Figure 145 Windows XP: Advanced TCP/IP Properties

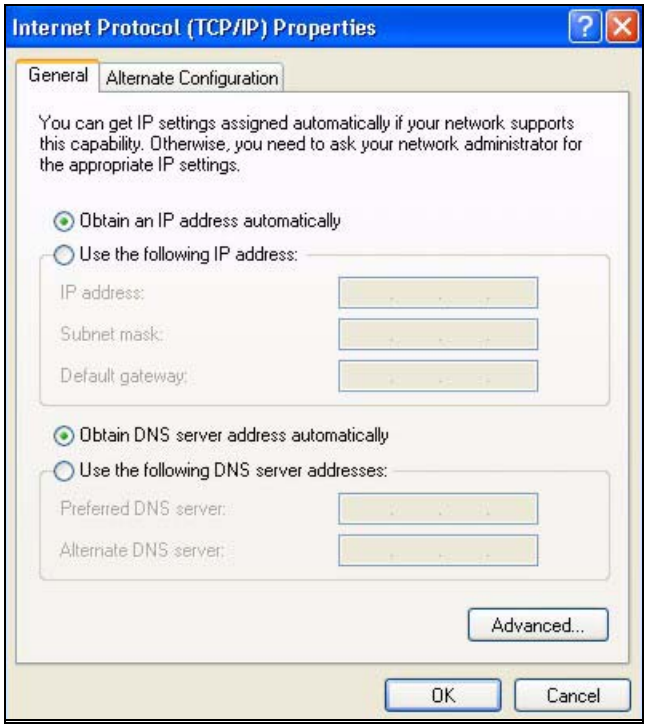


7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 146 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

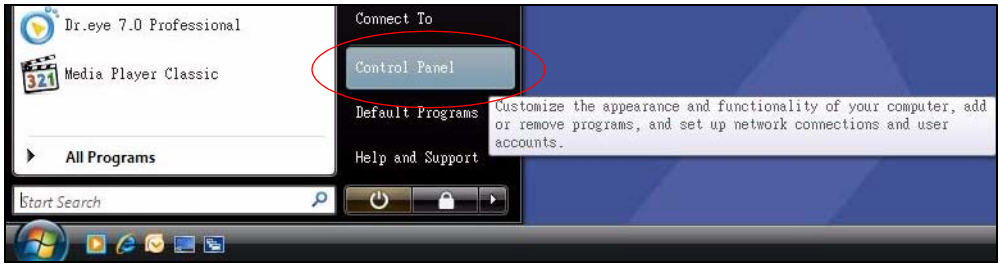
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Windows Vista

This section shows screens from Windows Vista Enterprise Version 6.0.

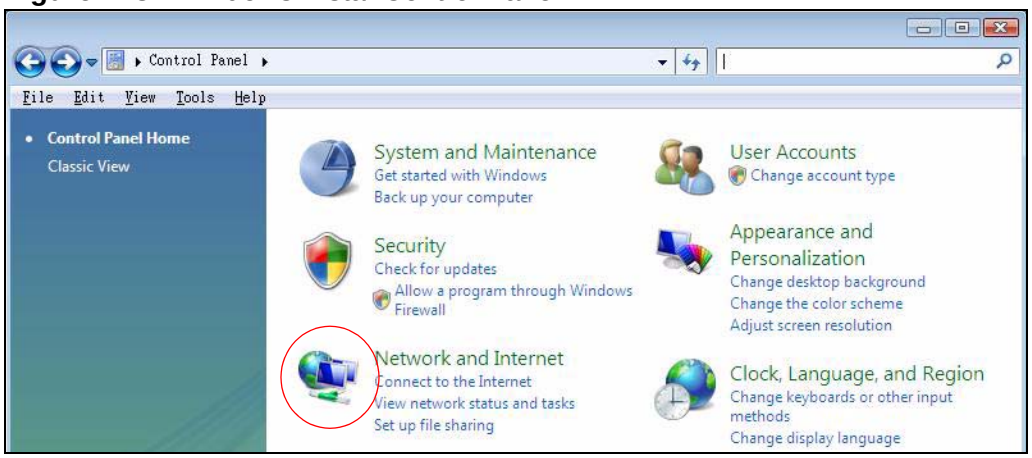
1 Click the **Start** icon, **Control Panel**.

Figure 147 Windows Vista: Start Menu


Dr.eye 7.0 Professional
Media Player Classic
All Programs
Start Search
Connect To
Control Panel
Default Programs
Help and Support
Customize the appearance and functionality of your computer, add or remove programs, and set up network connections and user accounts.

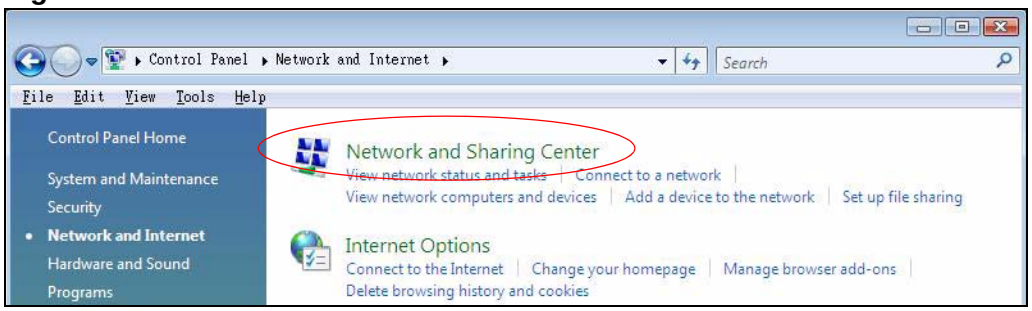
2 In the **Control Panel**, double-click **Network and Internet**.

Figure 148 Windows Vista: Control Panel



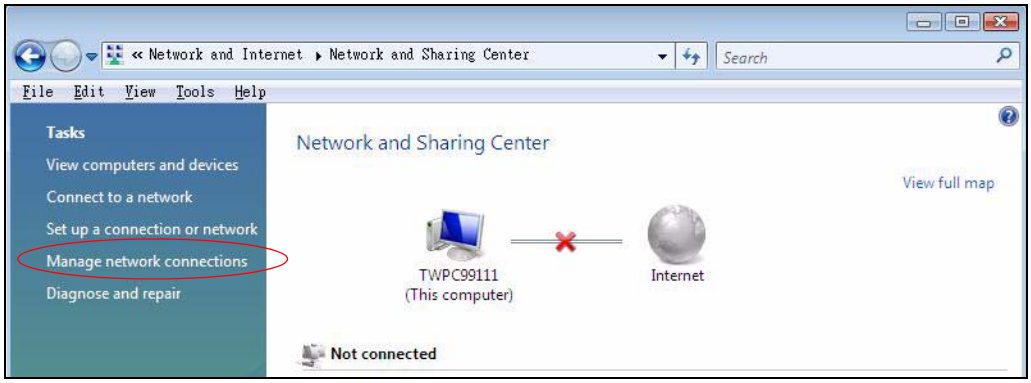
3 Click **Network and Sharing Center**.

Figure 149 Windows Vista: Network And Internet



4 Click **Manage network connections**.

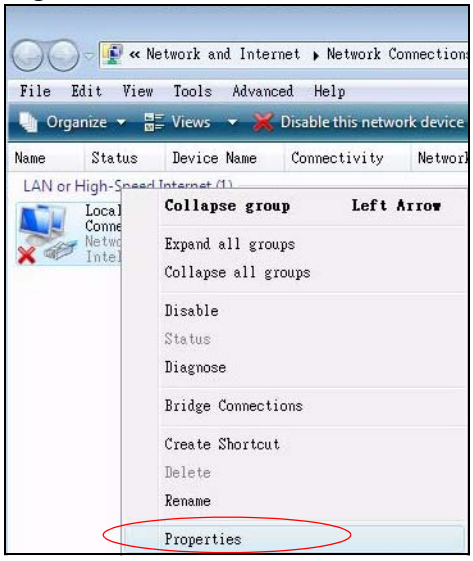
Figure 150 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then click **Properties**.

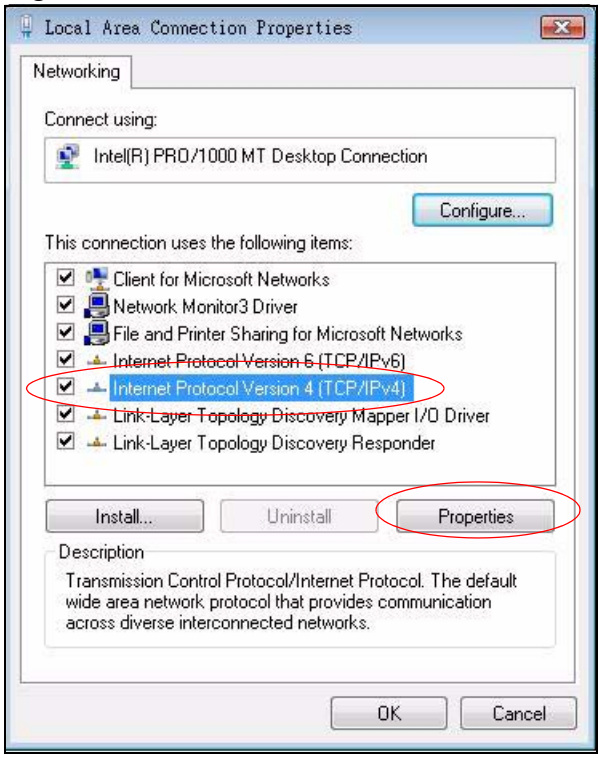
Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

Figure 151 Windows Vista: Network and Sharing Center



6 Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

Figure 152 Windows Vista: Local Area Connection Properties

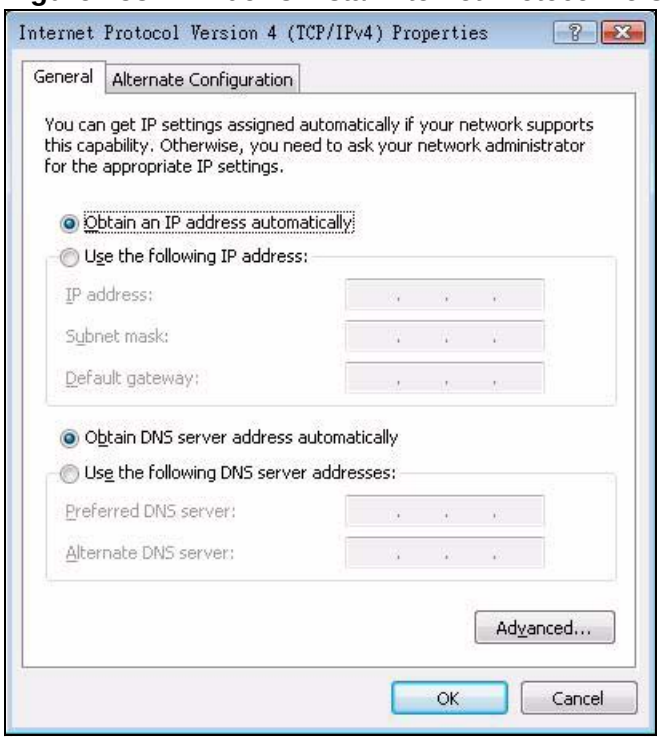


7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens (the **General tab**).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

- Click **Advanced**.

Figure 153 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

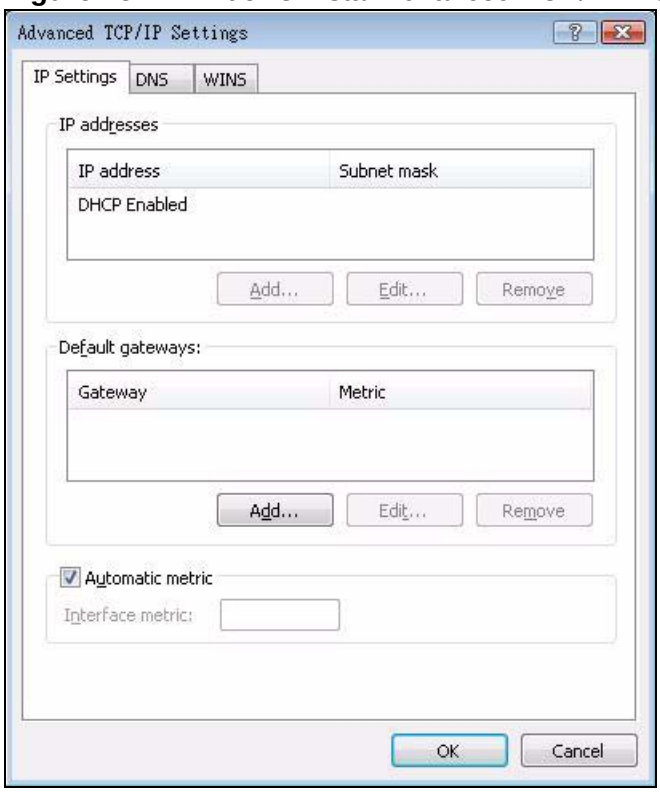
8 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

Figure 154 Windows Vista: Advanced TCP/IP Properties

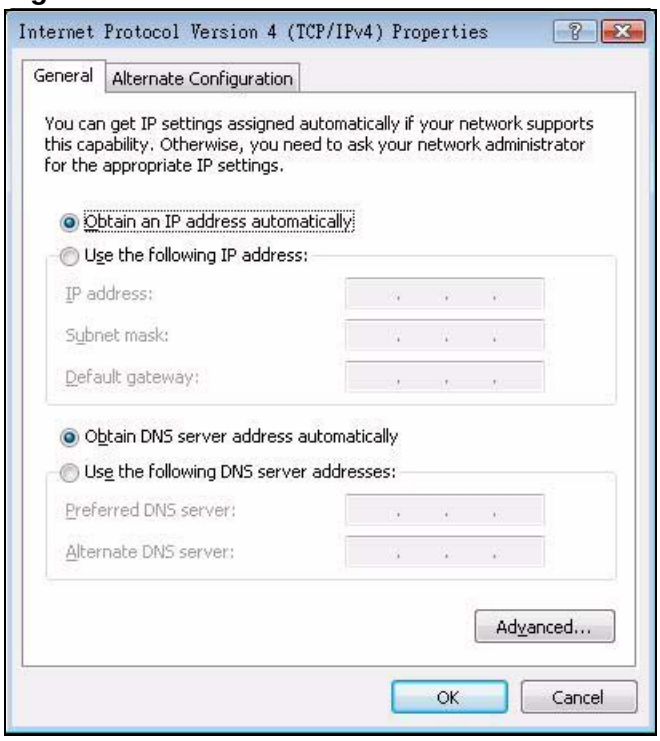


9 In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, (the **General tab**):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 155 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

10 Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

11 Click **Close** to close the **Local Area Connection Properties** window.

12 Close the **Network Connections** window.

13 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

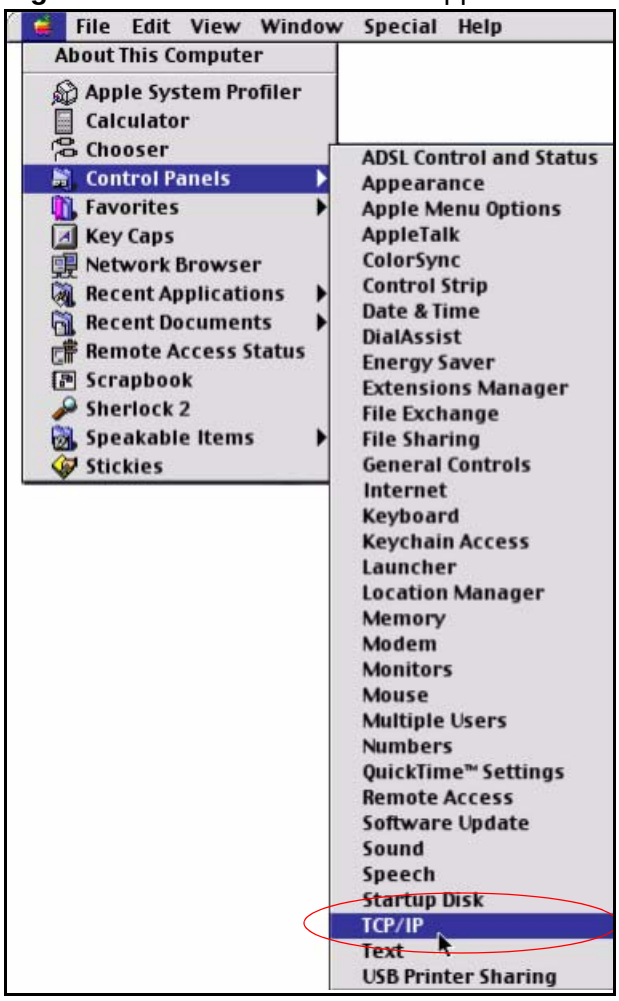
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

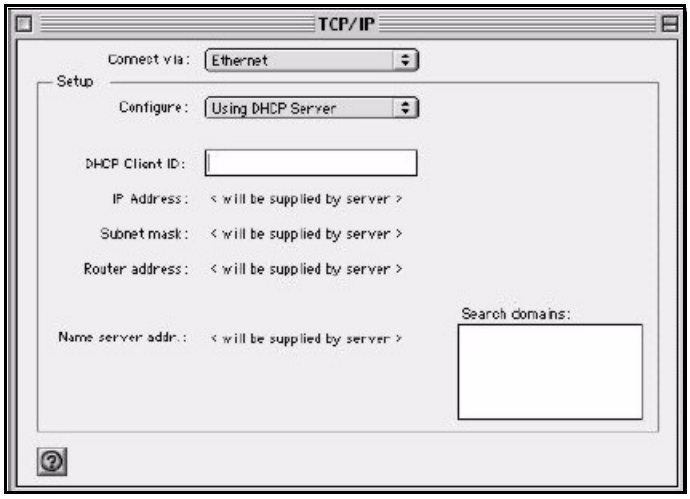
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 156 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 157 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

5 Close the **TCP / IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your ZyXEL Device and restart your computer (if prompted).

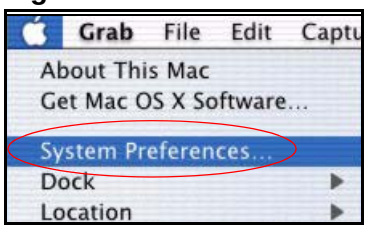
Verifying Settings

Check your TCP/IP properties in the **TCP / IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 158 Macintosh OS X: Apple Menu

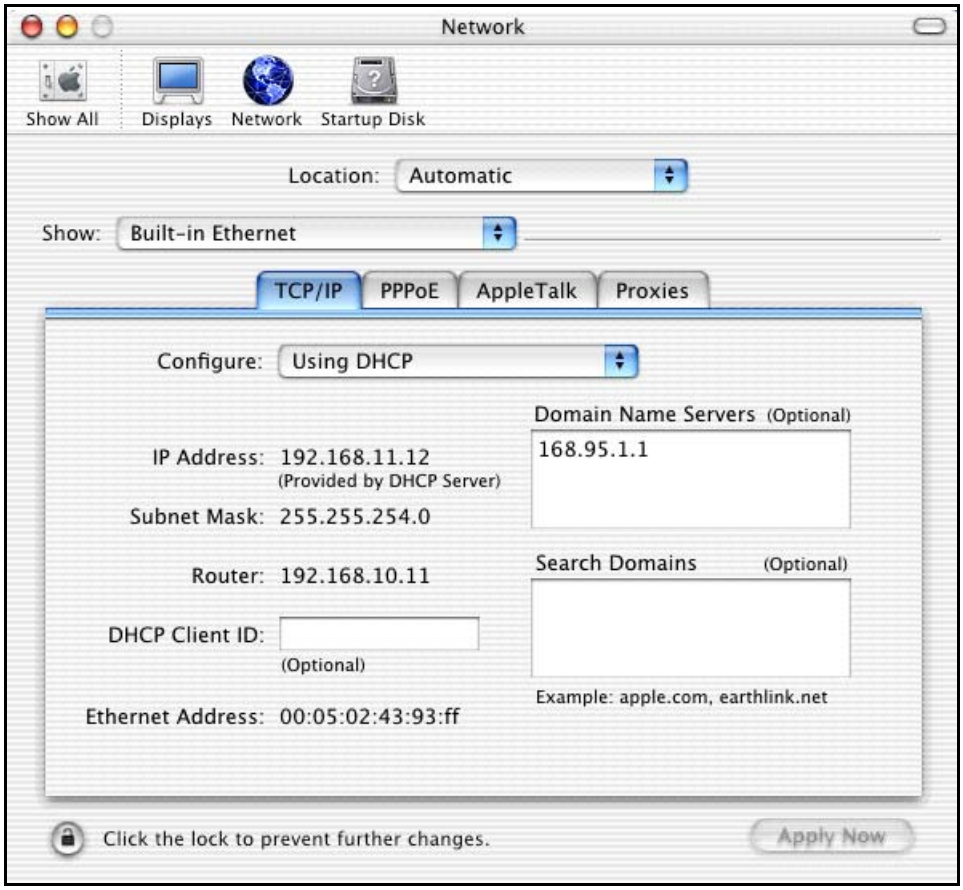


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 159 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

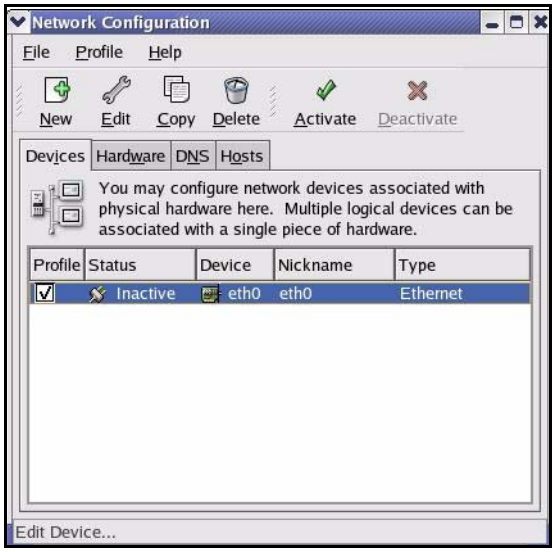
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 160 Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

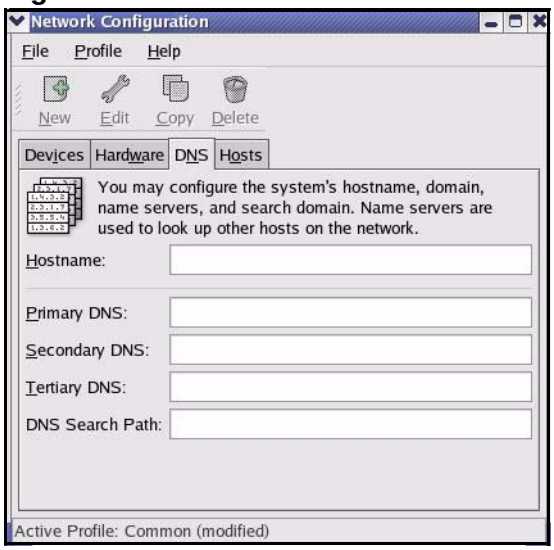
Figure 161 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 162 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 163 Red Hat 9.0: KDE: Network Configuration: Activate

Question
redhat-config-network:
You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.
Do you want to continue?
No
Yes

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 164 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the BOOTPROTO= field. Type IPADDR= followed by the IP address (in dotted decimal notation) and type NETMASK= followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 165 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the resolv.conf file in the /etc directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 166 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter ./network restart in the /etc/rc.d/init.d directory. The following figure shows an example.

Figure 167 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 168 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

B

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

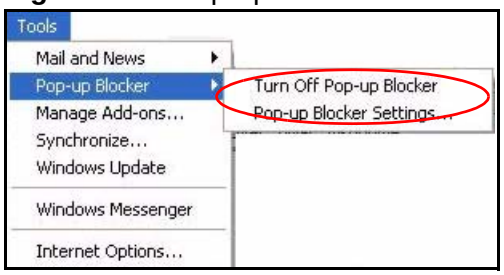
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 169 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 170 Internet Options: Privacy

3 Click **Apply** to save this setting.

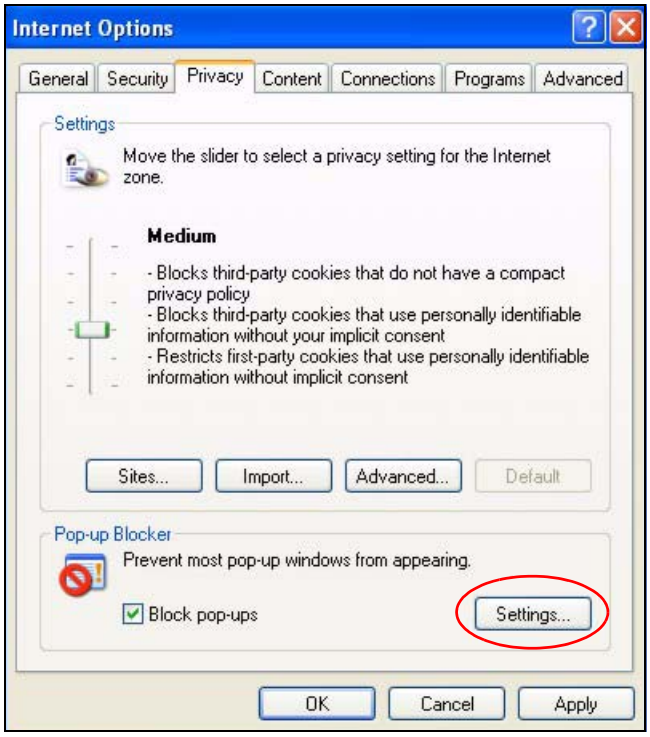
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 171 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 172 Pop-up Blocker Settings

Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

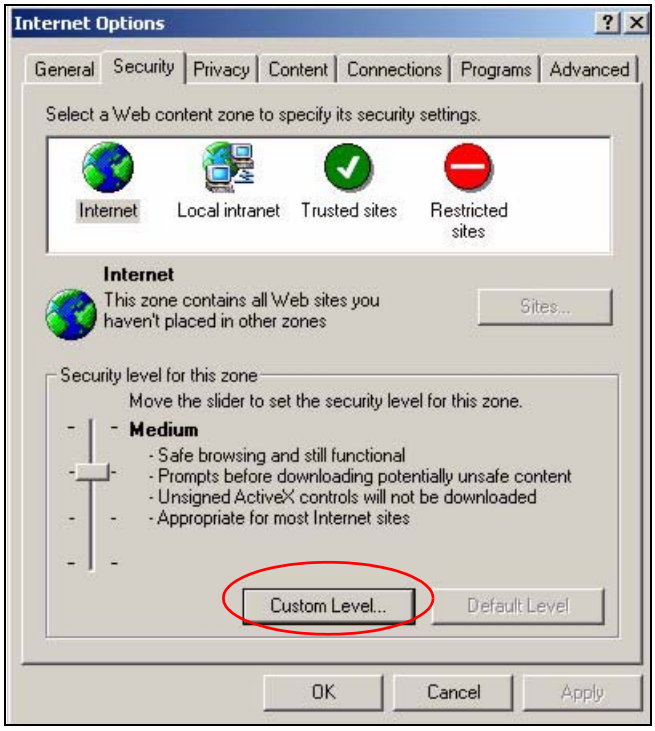
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 173 Internet Options: Security



2 Click the **Custom Level...** button.

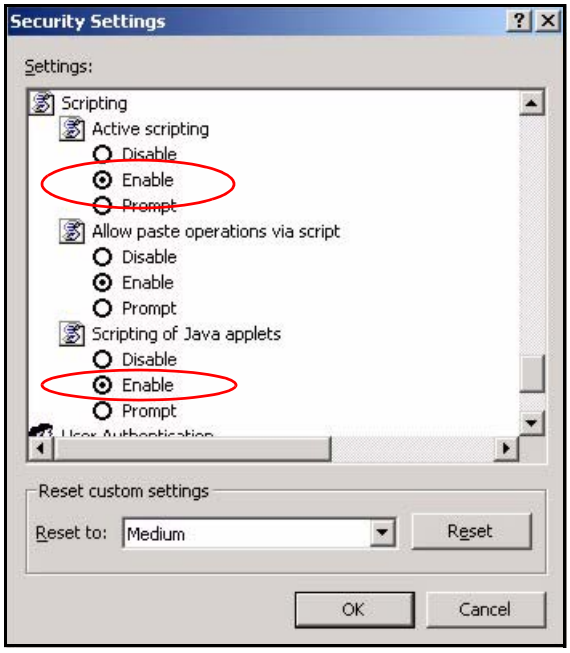
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 174 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

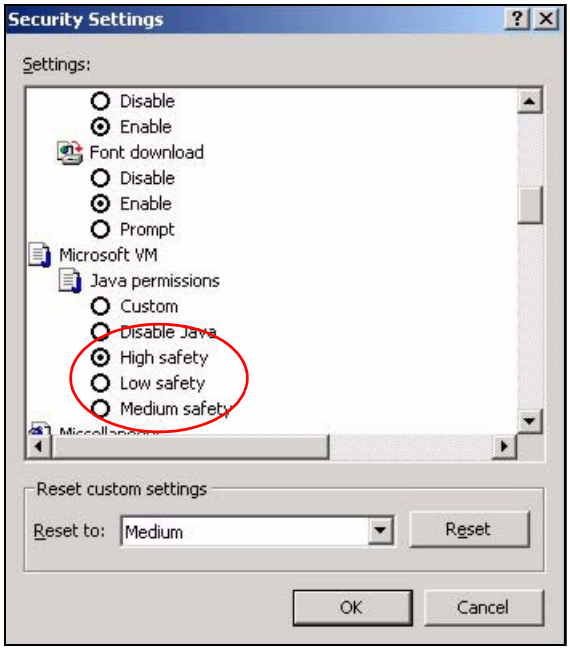
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 175 Security Settings - Java



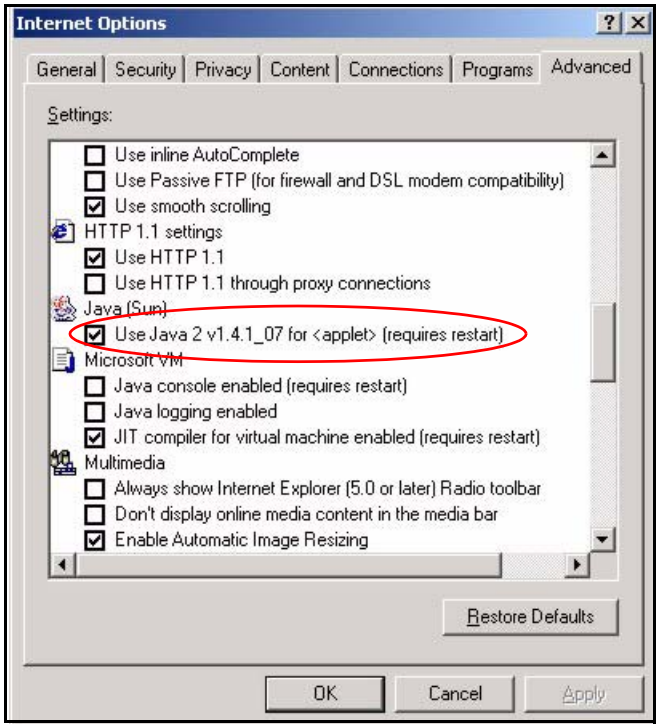
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 176 Java (Sun)

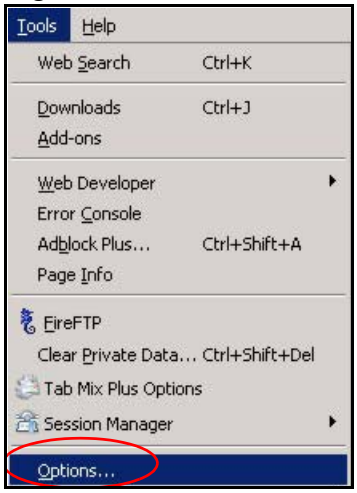


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

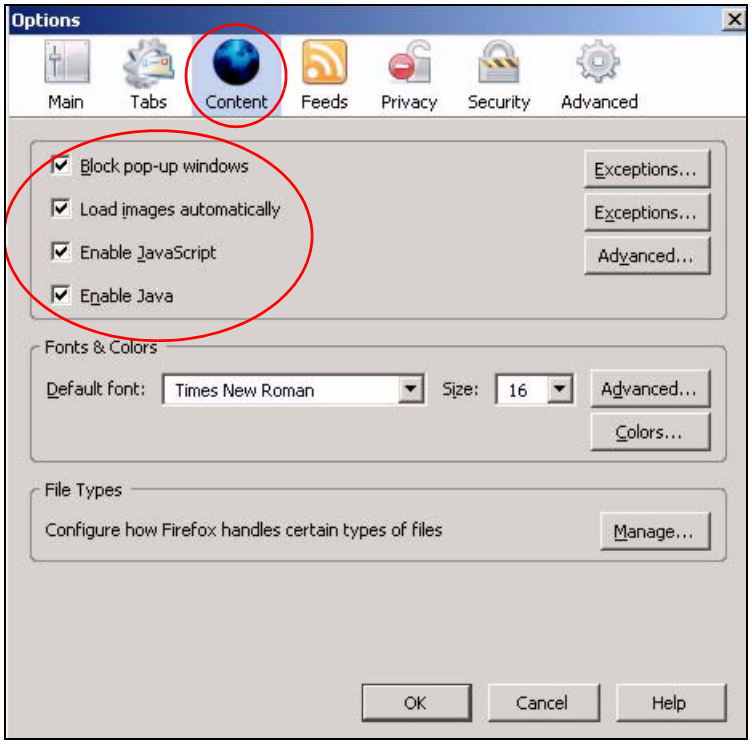
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 177 Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 178 Mozilla Firefox Content Security



C

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

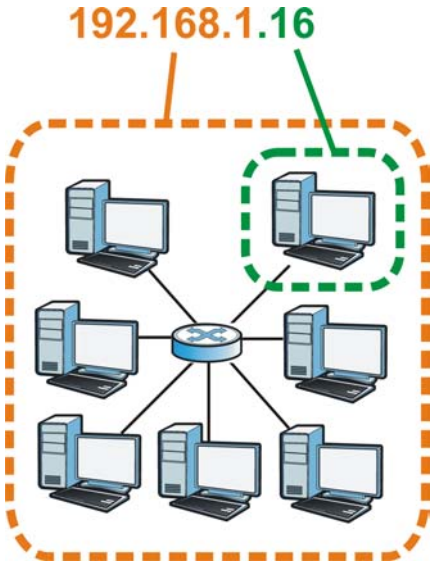
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 179 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 118 Subnet Masks

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 119 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 120 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} – 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} – 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} – 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} – 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 121 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

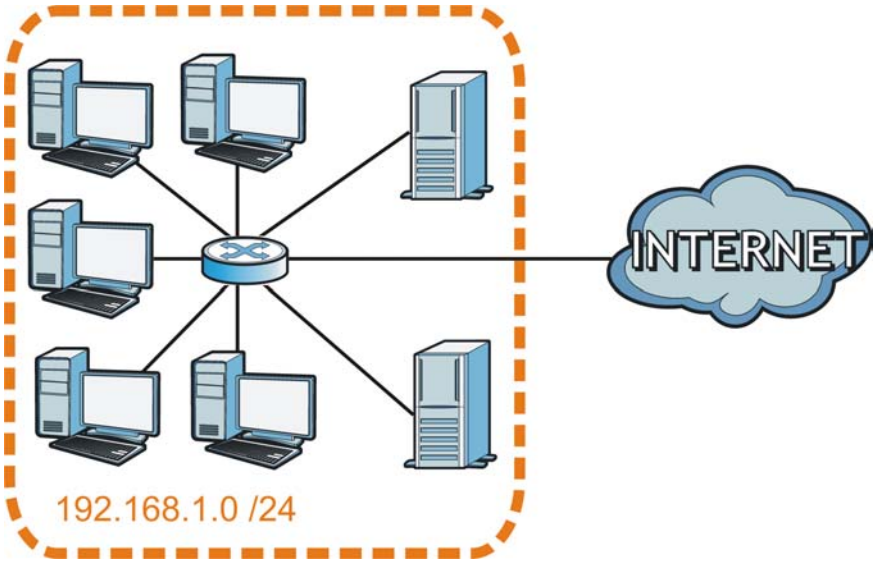
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 180 Subnetting Example: Before Subnetting

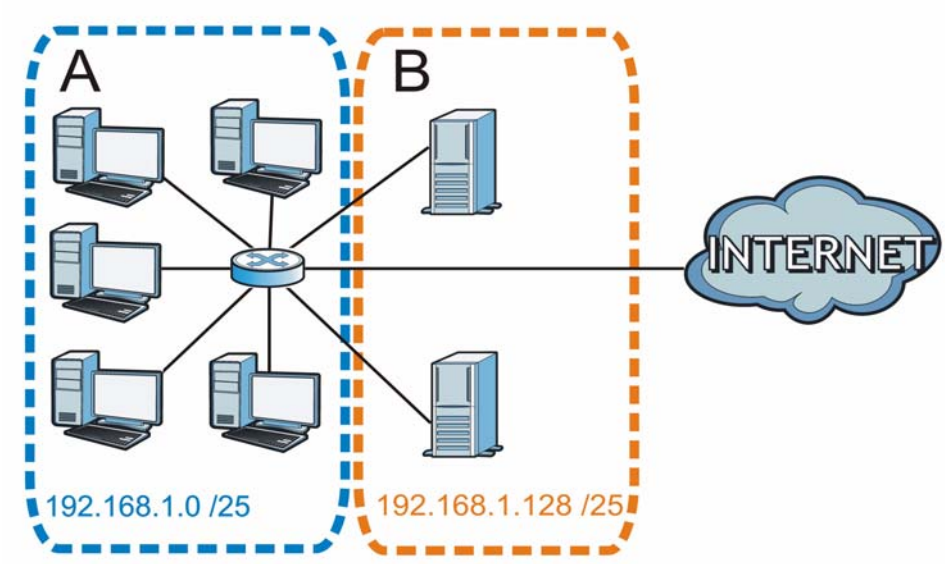


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 181 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 122 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 123 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 124 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 125 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 126 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 127 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 128 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP

addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

D

Wireless LANs

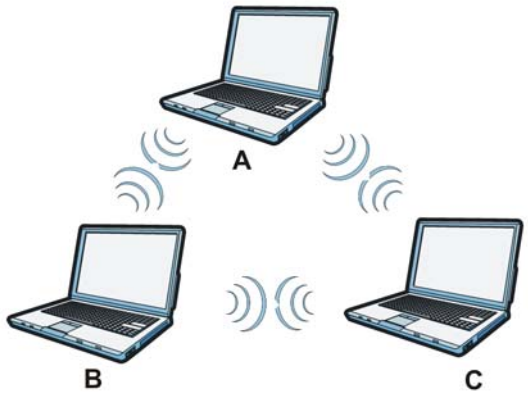
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 182 Peer-to-Peer Communication in an Ad-hoc Network



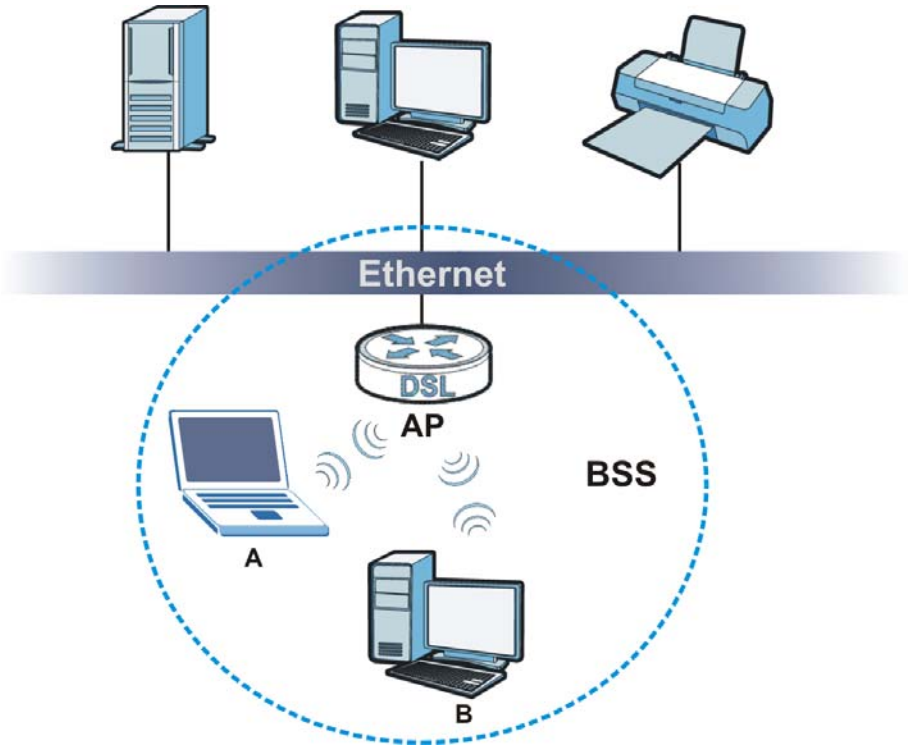
BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate

with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 183 Basic Service Set



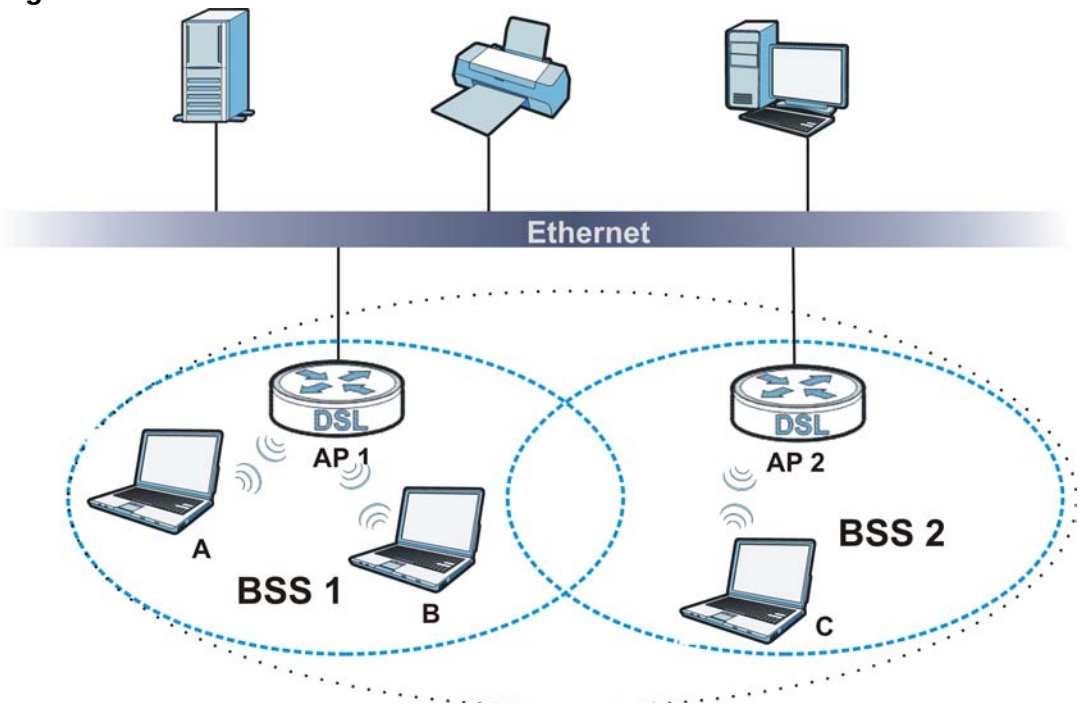
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 184 Infrastructure WLAN



Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

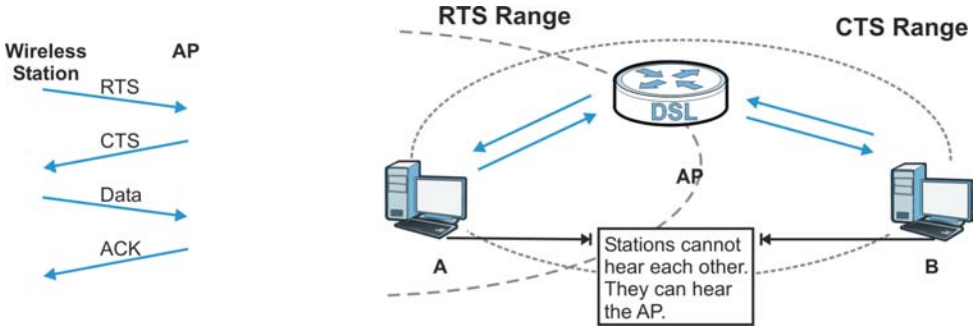
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or

wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 185 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the ZyXEL Device uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has

several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 129 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/ 48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the ZyXEL Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyXEL Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device.

Table 130 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 131 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption

keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

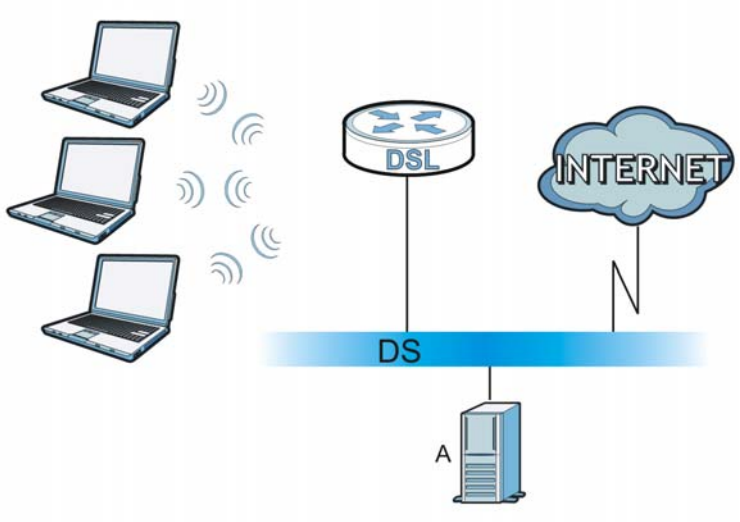
WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 186 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

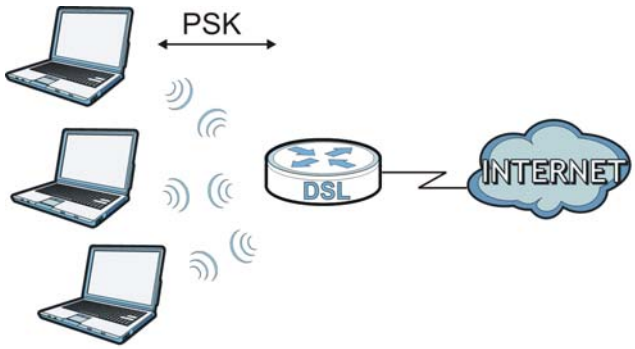
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 187 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 132 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

E

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 133 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.

Table 133 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.

Table 133 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

F

Legal Information

Copyright

Copyright © 2009 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.

- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 !

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or

purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Index

Numbers

802.1Q/1P 243
  activation 249
  example 245
  group settings 250
  management VLAN 249
  port settings 252
  priority 243, 252
  PVC 244
  PVID 252
  tagging frames 244, 251

A

activation
  802.1Q/1P 249
  Any IP 115
  classifiers 260
  content filtering 208
  dynamic DNS 276
  DYNDNS wildcard 276
  MAC address filter 140
  NAT 165
  port forwarding 169
  protocol filters 213
  QoS 259
  SIP ALG 173
  SSID 141
  static route 237, 240
  UPnP 291
  wireless LAN 132
    scheduling 147
  WPS 143
address mapping 169
  rules 171
  types 171, 172, 176
Address Resolution Protocol, see ARP
administrator password 305
alerts 309
  firewalls 193
algorithm, certificates 228
  MD5 fingerprint 228
  SHA1 fingerprint 228
alternative subnet mask notation 398
antenna
  directional 420
  gain 419
  omni-directional 420
anti-probing 182
Any IP 115, 125
  ARP 126
  example 125
  status 44
AP (access point) 407
applications, NAT 176
ARP 126
asymmetrical routes 188
ATM
  MBS 93, 100
  PCR 93, 100
  QoS 93, 100, 107
  SCR 93, 100
authentication 150, 151
  RADIUS server 152
  WPA 137

B

backup
  configuration 328, 329, 333
backup type 102
Basic Service Set, See BSS 405
Basic Service Set, see BSS
broadcast 88
BSS 153, 405
  example 154

C

CA 223, 413
  algorithm 228
  trusted 224, 227
CBR 93, 100, 107
Certificate Authority
  See CA.
certificates 223, 229
  advantages 229
  algorithm 228
  CA 223
    trusted 224, 227
  example 223
  exporting 228
  formats 224
  PEM 228
Certification Authority, see CA
certifications 425
  notices 427
  viewing 427
channel 407
  interference 407
channel, wireless LAN 149
Class of Service, see CoS
classifiers 260
  802.1Q tags 263
  activation 260
  configuration 261, 268
  creation 260
  DSCP 262, 264
  FTP 264
  priority 262
  remote node 264
  routing policy 262
  SIP 264
CLI 24
client list 118
Command Line Interface, see CLI
compatibility, WDS 145
configuration 333
  backup 328, 329, 333
  classifiers 261, 268
  DHCP 117
  file 324
  firewalls 187, 191, 198
  IP alias 120
  logs 311
  packet filtering 214
  port forwarding 167
  reset 335
  restoring 325, 334
  WAN 89
  wireless LAN 131
connection
  nailed-up 98, 105
  on demand 98
content filtering 205
  activation 208
  example 206
  keywords 208
  schedules 209
  trusted IP addresses 210
  URL 205
copyright 425
CoS 255
  DiffServ 271
creation
  classifiers 260
CTS (Clear to Send) 408
CTS threshold 138, 149
customized services 192, 193, 194

D

data fragment threshold 138, 150
default server, NAT 166, 168
Denials of Service, see DoS
DHCP 112, 117, 122, 303
Differentiated Services, see DiffServ
DiffServ 271
DiffServ Code Point, see DSCP
disclaimer 425
DNS 91, 112, 117, 122, 286
Domain Name System, see DNS
DoS 182
  three-way handshake 197
  thresholds 182, 197, 198, 199
DSCP 262, 264, 271
dynamic DNS 275
  activation 276
  wildcard 275

activation 276
Dynamic Host Configuration Protocol, see DHCP
dynamic WEP key exchange 414
DYNDNS wildcard 275
activation 276

E

EAP Authentication 412
e-mail logs 312
encapsulation 87, 90, 97
ENET ENCAP 103
PPPoA 104
PPPoE 103
RFC 1483 104
encryption 132, 152, 415
WEP 134
key 134
WPA 136
authentication 137
reauthentication 135, 137
WPA-PSK 135
pre-shared key 135
ENET ENCAP 90, 97, 103
ESS 406
exporting
trusted CA 228
Extended Service Set, See ESS 406

F

FCC interference statement 425
filters
content 205
activation 208
example 206
keywords 208
schedules 209
trusted IP addresses 210
URL 205
MAC address 139, 151
activation 140
packets 211
configuration 214
firewalls 219
generic filters 216
logs 215, 218
NAT 219
protocol filters 213
structure 211
types 212, 219
firewalls 181
actions 192
address types 192
alerts 193
anti-probing 182
asymmetrical routes 188
configuration 187, 191, 198
customized services 192, 193, 194
default action 188
DoS 182
thresholds 182, 197, 198, 199
example 182
half-open sessions 199
ICMP 182
logs 192
maximum incomplete 199
P2P 198
packet direction 188
packet filtering 219
rules 186
schedules 192
security 200
three-way handshake 197
triangle route 188, 201, 202
solutions 203
firmware 324, 331
upgrading 326
version 38
forwarding ports 164, 166
activation 169
configuration 167
example 167
rules 169
fragmentation threshold 138, 150, 409
FTP 24, 285
backing up configuration 328
limitations 325
QoS 264
restoring configuration 325, 326
upgrading firmware 326, 327

G

generic filters 216, 219
length 218
logs 218
mask 218
offset 218

H

half-open sessions 199
hidden node 407

I

IANA 403
Internet Assigned Numbers Authority
see IANA
IBSS 405
ICMP 182, 287
IEEE 802.11g 409
IGA 174
IGMP 88, 112, 115, 125
ILA 174
importing
trusted CA 225
Independent Basic Service Set
See IBSS 405
initialization vector (IV) 415
Inside Global Address, see IGA
Inside Local Address, see ILA
Internet Control Message Protocol, see ICMP
Internet Group Multicast Protocol, see IGMP
IP address 88, 91, 97, 105, 112, 123
ARP 126
default server 166, 168
private 123
IP alias 119
configuration 120
NAT applications 176
IP precedence 271

L

LAN 111
Any IP 115, 125
example 125
client list 118
DHCP 112, 117, 122
DNS 112, 117, 122
IGMP 112, 125
IP address 112, 113, 123
IP alias 119
configuration 120
MAC address 119, 238
multicast 112, 115, 124
NetBIOS 115
packet filter 115
RIP 112, 115, 120, 124
status 39
subnet mask 112, 113, 123
LEDs 26
limitations
FTP 325
wireless LAN 153
WPS 161
Local Area Network, see LAN
login 31
passwords 32
logs 309
alerts 309
e-mail 312
error messages 314
example 314
firewalls 192
generic filters 218
protocol filters 215
schedules 313
settings 311

M

MAC address 119, 140, 238
filter 130, 132, 139, 151
MAC address filter
activation 140
management VLAN 249
mapping address 169

rules 171
types 171, 172, 176
Maximum Burst Size, see MBS
maximum incomplete 199
Maximum Transmission Unit, see MTU
MBS 93, 100, 107
MBSSID 154
MD5 fingerprint 228
metric 106
monitor, QoS 267, 269
MTU 94, 100
multicast 88, 93, 99, 112, 115, 124
IGMPInternet Group Multicast Protocol, see IGMP
Multiple BSS, see MBSSID
multiplexing 91, 97, 104
LLC-based 105
VC-based 104

N

nailed-up connection 91, 98, 105
NAT 98, 163, 164, 173, 174, 403
activation 165
address mapping 169
rules 171
types 171, 172, 176
applications 176
IP alias 176
default server IP address 166, 168
example 175
global 174
IGA 174
ILA 174
inside 174
local 174
outside 174
P2P 165
packet filtering 219
port forwarding 164, 166
activation 169
configuration 167
example 167
rules 169
remote management 281
SIP ALG 173
activation 173
SUA 164, 165
NetBIOS 115
Network Address Translation
see NAT
Network Address Translation, see NAT
Network Basic Input/Output System

P

P2P 165, 198
packet direction 188
packet filter
LAN 115
structure 211
WAN 94, 100
packet filtering 211
configuration 214
firewalls 219
generic filters 216
NAT 219
protocol filters 213
types 212, 219
packet filters
logs 215, 218
packet statistics 45
Pairwise Master Key (PMK) 415, 417
passthrough, PPPoE 94
passwords 32
administrator 305
PBC 156
PCR 93, 100, 107
Peak Cell Rate, see PCR
PEM 228
PIN, WPS 143, 145, 156
example 158
port forwarding 164, 166
activation 169
configuration 167
example 167
rules 169
PPPoA 90, 97, 104
PPPoE 90, 97, 103
passthrough 94
preamble 138, 149

preamble mode 409
pre-shared key 135
private IP address 123
probing, firewalls 182
product registration 428
protocol filters 213, 219
  activation 213
  logs 215
PSK 415
public-private key pairs 229
push button 27, 145
Push Button Configuration, see PBC
push button, WPS 156
PVC 244
PVID 252

Q

QoS 253
  802.1Q tags 263, 270
  activation 259
  classifiers 260
    activation 260
    configuration 261, 268
    creation 260
    priority 262
  CoS 255
  DiffServ 271
  DSCP 262, 264, 271
  example 255
  FTP 264
  IP precedence 271
  monitor 267, 269
  priority queue 272
  remote node 264
  routing policy 262
  SIP 264
Quality of Service, see QoS
Queue Setup 267

R

RADIUS 411
  message types 411
  messages 411
  shared secret key 412
RADIUS server 152
reauthentication, WPA 135, 137
registration
  product 428
related documentation 3
remote management 279
  DNS 286
  FTP 285
  ICMP 287
  limitations 280
  NAT 281
  Telnet 284
  WWW 283
remote node 264
reset 27, 335
restart 336
restoring configuration 325, 334
restrictions
  FTP 325
RFC 1483 90, 97, 104
RIP 93, 99, 112, 115, 120, 124
Routing Information Protocol, see RIP
routing policy 262
RTS (Request To Send) 408
  threshold 407, 408
RTS threshold 138, 149
rules, port forwarding 169

S

safety warnings 8
schedules
  content filtering 209
  firewalls 192
  logs 313
  wireless LAN 147
SCR 93, 100, 107
security
  network 200
  wireless LAN 132, 150
Service Set IDentifier, see SSID
Session Initiation Protocol, see SIP

setup 333
classifiers 261, 268
DHCP 117
firewalls 187, 191, 198
IP alias 120
logs 311
packet filtering 214
port forwarding 167
WAN 89
wireless LAN 131
SHA1 fingerprint 228
shaping traffic 106, 107
Single User Account, see SUA
SIP ALG 173, 264
activation 173
SSID 130, 132, 142, 151
activation 141
MBSSID 154
static route 239
activation 237, 240
example 239
Statistics 339
status 34, 37
Any IP 44
firmware version 38
LAN 39
packet statistics 45
WAN 39
wireless LAN 40
WLAN 43
WPS 143
SUA 164, 165
subnet 395
subnet mask 112, 123, 396
subnetting 398
Sustain Cell Rate, see SCR
syntax conventions 6
system 304
backing up configuration 329
backup configuration 328
firmware 324, 331
upgrading 326
version 38
LED 26
name 305
passwords 32
administrator 305
reset 27
restoring configuration 325
status 34, 37
LAN 39
WAN 39
wireless LAN 40
time 306

T

tagging frames 244, 251
Telnet 284
TFTP 329
backing up configuration 329
upgrading firmware 327
three-way handshake 197
thresholds
data fragment 138, 150
DoS 182, 197, 198, 199
P2P 198
RTS/CTS 138, 149
time 306
TR-069 24
trademarks 425
traffic priority 243, 252
traffic redirect 102, 109
traffic shaping 106
example 107
triangle route 188, 201, 202
solutions 203
trusted CA 224, 227
algorithm 228
exporting 228
importing 225
MD5 fingerprint 228
PEM 228
SHA1 fingerprint 228

U

UBR 93, 100, 108
unicast 88
Universal Plug and Play, see UPnP
upgrading firmware 326, 331

UPnP 289
activation 291
cautions 290
example 292
installation 292
NAT traversal 289
URL 205

V

VBR 108
VBR-nRT 93, 100, 108
VBR-RT 93, 100, 108
VCI 91, 97, 105
Virtual Channel Identifier, see VCI
Virtual Local Area Network, see VLAN
Virtual Path Identifier, see VPI
VLAN 243
802.1P priority 243, 252
activation 249
example 245
group settings 250
management group 249
port settings 252
PVC 244
PVID 252
tagging frames 244, 251
VPI 91, 97, 105

W

WAN 87
ATM QoS 93, 100, 107
DNS 91
encapsulation 87, 90, 97
IGMP 88
IP address 88, 91, 97, 105
mode 90, 97
modulation 90
MTU 94, 100
multicast 88, 93, 99
multiplexing 91, 97, 104
nailed-up connection 91, 98, 105
NAT 98
packet filter 94, 100
RIP 93, 99
setup 89
status 39
traffic shaping 106
example 107
VCI 91, 97, 105
VPI 91, 97, 105
warranty 427
note 427
WDS 145, 155
compatibility 145
example 155
web configurator 24, 31
login 31
passwords 32
WEP 134, 152
key 134
Wide Area Network, see WAN
Wi-Fi Protected Access 414
WiFi Protected Setup, see WPS
wireless client WPA supplicants 416
Wireless Distribution System, see WDS
wireless LAN 129, 148
activation 132
authentication 150, 151
BSS 153
example 154
channel 149
configuration 131
encryption 132, 152
example 148
fragmentation threshold 138, 150
limitations 153
MAC address filter 130, 132, 139, 140, 151
MBSSID 154
preamble 138, 149
RADIUS server 152
RTS/CTS threshold 138, 149
scheduling 147
security 150
SSID 130, 132, 142, 151
activation 141
status 40
WDS 145, 155
compatibility 145
example 155
WEP 134, 152
key 134

WPA 136, 152
authentication 137
reauthentication 135, 137
WPA-PSK 135, 152
pre-shared key 135
WPS 143, 155, 158
activation 143
adding stations 145
example 160
limitations 161
PIN 143, 145, 156
push button 27, 145, 156
status 143
wireless security 410
Wireless tutorial 49
WLAN
interference 407
security parameters 418
WPA 136, 152, 414
authentication 137
key caching 416
pre-authentication 416
reauthentication 135, 137
user authentication 416
vs WPA-PSK 415
wireless client supplicant 416
with RADIUS application example 416
WPA2 414
user authentication 416
vs WPA2-PSK 415
wireless client supplicant 416
with RADIUS application example 416
WPA2-Pre-Shared Key 414
WPA2-PSK 414, 415
application example 417
WPA-PSK 135, 152, 415
application example 417
pre-shared key 135
WPS 143, 155, 158
activation 143
adding stations 145
example 160
limitations 161
PIN 143, 145, 156
example 158
push button 27, 145, 156
status 143

Z

zero configuration Internet access 108